ISSN 1725-2466

Gazzetta ufficiale C 128

dell'Unione europea

Edizione in lingua italiana

Comunicazioni ed informazioni

52° anno

6 giugno 2009

Numero d'informazione Sommario Pagina

I *Risoluzioni, raccomandazioni e pareri*

PARERI

Garante europeo della protezione dei dati

2009/C 128/01 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 1

2009/C 128/02 Parere del garante europeo della protezione dei dati (GEPD) sulla comunicazione della Commissione al Consiglio, al Parlamento europeo e al Comitato economico e sociale europeo dal titolo «Verso una strategia europea in materia di giustizia elettronica» 13

2009/C 128/03 Progetto di parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera 20

2009/C 128/04 Secondo parere del Garante europeo della protezione dei dati sulla revisione della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) 28

2009/C 128/05 Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Consiglio che stabilisce l'obbligo per gli Stati membri di mantenere un livello minimo di scorte di petrolio greggio e/o di prodotti petroliferi 42

IT

(segue)

IV *Informazioni*

INFORMAZIONI PROVENIENTI DALLE ISTITUZIONI E DAGLI ORGANI DELL'UNIONE EUROPEA

Commissione

2009/C 128/06 Tassi di cambio dell'euro 45

Rettifiche

2009/C 128/07 Rettifica del tasso di interesse applicato dalla Banca centrale europea alle sue principali operazioni di rifinanziamento *(GU C 124 del 4 giugno 2009)* 46

IT

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

Parere del garante europeo della protezione dei dati (GEPD) sulla comunicazione della Commissione al Consiglio, al Parlamento europeo e al Comitato economico e sociale europeo dal titolo «Verso una strategia europea in materia di giustizia elettronica»

(2009/C 128/02)

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 [1],

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 [2], in particolare l'articolo 41,

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE

1. Il 30 maggio 2008 è stata adottata la comunicazione della Commissione al Consiglio, al Parlamento europeo e al Comitato economico e sociale europeo dal titolo «Verso una strategia europea in materia di giustizia elettronica» (nel seguito «la comunicazione»). Conformemente all'articolo 41 del regolamento (CE) n. 45/2001, il GEPD presenta il seguente parere.

2. La comunicazione propone una strategia in materia di giustizia elettronica che si prefigge di accrescere la fiducia dei cittadini nello spazio europeo di giustizia Il primo obiettivo della giustizia elettronica dovrebbe essere quello di potenziare l'efficacia della giustizia ovunque in Europa, a vantaggio dei cittadini L'azione dell'Unione europea dovrebbe permettere ai cittadini di accedere all'informazione superando le barriere linguistiche, culturali e giuridiche derivanti dalla molteplicità degli ordinamenti. La comunicazione contiene in allegato una proposta di piano d'azione e di calendario per i vari progetti.

3. Nel presente parere il GEPD commenta la comunicazione relativamente al trattamento di dati personali, alla tutela della vita privata libera nelle comunicazioni elettroniche e alla libera circolazione di tali dati.

II. ANTEFATTO E CONTESTO

4. Nel giugno del 2007 il Consiglio GAI [3] aveva identificato alcune priorità per lo sviluppo della giustizia elettronica:

— istituzione di un'interfaccia europea (portale «Giustizia elettronica»);

— creazione delle condizioni per il collegamento in rete di vari registri, ad esempio casellari giudiziali, registri d'insolvenza, registri delle imprese e catasti;

— avvio dei preparativi per l'uso delle TI per il procedimento europeo d'ingiunzione di pagamento;

— miglioramento dell'uso della tecnologia della videoconferenza per comunicare nel quadro dei procedimenti transfrontalieri, in particolare riguardo all'assunzione delle prove;

— concezione di strumenti di ausilio alla traduzione e all'interpretazione.

5. Da allora i lavori sulla giustizia elettronica sono progrediti di buon passo. Secondo la Commissione i lavori svolti in questo contesto devono assegnare priorità ai progetti operativi e alle strutture decentrate, garantendo nel contempo il coordinamento a livello europeo, basandosi sugli strumenti giuridici vigenti e avvalendosi degli strumenti informatici per accrescerne l'efficacia. Anche il Parlamento europeo ha espresso il suo sostegno al progetto di giustizia elettronica [4].

6. La Commissione ha sempre incoraggiato l'uso delle moderne tecnologie dell'informazione nel campo sia civile che penale. Ciò ha condotto a strumenti come il procedimento europeo d'ingiunzione di pagamento. Dal 2003 la Commissione gestisce il portale della rete giudiziaria europea in materia civile e commerciale, accessibile ai cittadini in 22 lingue. La Commissione ha anche ideato e istituito l'atlante giudiziario europeo. Questi strumenti sono elementi precursori di un futuro quadro europeo in materia di giustizia elettronica. Nel settore penale la Commissione ha elaborando uno strumento che consenta lo scambio delle informazioni estratte dai casellari giudiziari degli Stati membri [5]. Non solo la Commissione ma anche Eurojust ha sviluppato sistemi di comunicazione sicuri con le autorità nazionali.

[1] GU L 281 del 23.11.1995, pag. 31.
[2] GU L 8 del 12.1.2001, pag. 1.
[3] Doc. 10393/07 JURINFO 21.
[4] V. progetto di relazione del Parlamento europeo, Commissione giuridica.
[5] Si veda, in particolare, il sistema ECRIS citato nel seguito.

7. Nei prossimi anni la giustizia elettronica intende offrire molte opportunità per rendere lo spazio giudiziario europeo una realtà concreta per i cittadini. Onde mettere a punto una strategia globale in questa materia importante, la Commissione ha adottato la comunicazione in questione sulla giustizia elettronica, che fissa criteri obiettivi per individuare le priorità, in particolare per i progetti futuri a livello europeo, affinché si riescano a ottenere risultati concreti entro termini ragionevoli.

8. Il documento di lavoro dei servizi della Commissione, che accompagna la comunicazione con una sintesi della valutazione d'impatto, fornisce altresì alcune informazioni di base ([6]). La relazione sulla valutazione d'impatto è stata preparata considerando le reazioni di Stati membri, autorità giudiziarie, professioni legali, cittadini e imprese. Il GEPD non è stato consultato. La valutazione d'impatto privilegia un'opzione politica per risolvere i problemi che combina la dimensione europea e la competenza nazionale. La comunicazione ha optato per questa opzione. La strategia si concentrerà sui seguenti elementi: uso della videoconferenza, creazione del portale «Giustizia elettronica», miglioramento degli ausili alla traduzione attraverso lo sviluppo di strumenti di traduzione automatica disponibili in linea, miglioramento della comunicazione tra autorità giudiziarie, maggiore interconnessione tra registri nazionali e strumenti in linea per i procedimenti europei (ad esempio, il procedimento europeo d'ingiunzione di pagamento).

9. Il GEPD condivide l'accento posto su questi elementi. In generale appoggia un approccio completo alla giustizia elettronica. Approva la triplice esigenza di migliorare l'accesso alla giustizia, la cooperazione tra autorità giudiziarie europee e l'efficacia del sistema giudiziario. Applicando questo approccio si coinvolgono varie istituzioni e vari soggetti:

— gli Stati membri, che hanno la responsabilità primaria di garantire sistemi giudiziari efficaci e degni di fiducia;

— la Commissione europea, quale guardiana dei trattati;

— le autorità giudiziarie degli Stati membri, che necessitano di strumenti di comunicazione più sofisticati, in particolare nei casi transnazionali;

— le professioni legali, i cittadini e le imprese, che chiedono un uso migliore degli strumenti informatici onde ottenere risposte più soddisfacenti alle esigenze di giustizia.

10. La comunicazione è strettamente legata alla proposta di decisione del Consiglio che istituisce il sistema europeo di informazione sui casellari giudiziari (ECRIS). Il 16 settembre 2008 il GEPD ha adottato un parere sulla proposta ([7]), che ha appoggiato, purché fossero presi in considerazione una serie di elementi. In particolare ha fatto presente che garanzie supplementari di protezione dei dati dovrebbero compensare la carenza attuale di un quadro giuridico completo sulla protezione dei dati nella cooperazione tra polizia e autorità giudiziarie. Ha pertanto sottolineato l'esigenza di un effettivo coordinamento nella supervisione della protezione dei dati del sistema, che coinvolge le autorità degli Stati membri e la Commissione in qualità di fornitori dell'infrastruttura di comunicazione comune.

11. Alcune raccomandazioni del parere che meritano di essere ricordate:

— occorrerebbe un riferimento a un elevato livello di protezione dei dati quale condizione preliminare all'adozione delle misure di esecuzione;

— dovrebbe essere chiarita la responsabilità della Commissione relativa all'infrastruttura comune del sistema, nonché l'applicabilità del regolamento (CE) n. 45/2001 per garantire meglio la certezza del diritto;

— la Commissione, e non gli Stati membri, dovrebbe essere altresì responsabile del software di interconnessione per accrescere l'efficacia dello scambio e consentire una migliore supervisione del sistema.

— occorrerebbe definire e circoscrivere precisamente l'uso della traduzione automatica, al fine di favorire la reciproca comprensione dei vari reati penali senza rischiare di compromettere la qualità delle informazioni trasmesse.

12. Queste raccomandazioni sono tuttora esplicative del contesto in cui sarà analizzata l'attuale proposta.

III. GLI SCAMBI DI INFORMAZIONE PREVISTI NELLA COMUNICAZIONE

13. La giustizia elettronica ha un campo di applicazione molto esteso, comprendente di norma l'uso di tecnologie dell'informazione e della comunicazione (TIC) nell'amministrazione della giustizia all'interno dell'Unione europea. Sono inclusi diversi aspetti, quali progetti che forniscono in modo più efficace informazioni alle parti in un procedimento giudiziario. Tra questi aspetti figurano informazioni

([6]) Documento di lavoro dei servizi della Commissione che accompagna la comunicazione al Consiglio, al Parlamento Europeo e al Comitato economico e sociale europeo «Verso una strategia europea in materia di giustizia elettronica» — Sintesi della valutazione d'impatto, del 30.5.2008, SEC(2008) 1944.

([7]) Si veda il parere del GEPD sulla proposta di decisione del Consiglio che istituisce il sistema europeo di informazione sui casellari giudiziari (ECRIS) in applicazione dell'articolo 11 della decisione quadro 2008/XX/GAI, consultabile sul sito web del GEPD, www.edps.europa.eu, «consultation» e quindi «opinions», «2008».

in rete sui sistemi giudiziari, sulla legislazione e sulla giurisprudenza, sistemi di comunicazione elettronica che collegano le parti e gli organi giurisdizionali e l'elaborazione di procedure completamente elettroniche. Sono altresì compresi progetti europei quali l'uso di mezzi elettronici di registrazione delle udienze e progetti di scambio di informazioni o di interconnessione.

14. Anche se il campo di applicazione è molto esteso, il GEPD ha constatato che il portale conterrà informazioni sui procedimenti penali e sui sistemi giudiziari civile e commerciale, ma non su quelli amministrativi. Ci sarà inoltre un collegamento ad un atlante giudiziario in materia civile e penale, ma non in materia amministrativa, anche se sarebbe auspicabile che i cittadini e le imprese potessero accedere a sistemi di giustizia amministrativa, ossia al diritto amministrativo e alle procedure di ricorso. Dovrebbe essere previsto anche un collegamento all'Associazione dei Consigli di Stato. Queste aggiunte consentirebbero ai cittadini di muoversi più agevolmente sul terreno spesso intricato del diritto amministrativo con tutti i suoi organi giurisdizionali, per essere maggiormente informati riguardo ai sistemi giudiziari amministrativi.

15. Il GEPD raccomanda pertanto di inserire le procedure amministrative nella giustizia elettronica. In questo contesto, si dovrebbero avviare progetti di giustizia elettronica intesi a rafforzare la visibilità delle norme sulla protezione dei dati e delle autorità nazionali garanti della protezione dei dati, segnatamente in relazione ai tipi di dati trattati nel quadro di giustizia elettronica, in linea con la cosiddetta «iniziativa di Londra» avviata nel novembre 2006 dalle autorità garanti della protezione dei dati e volta a «comunicare e a rendere più efficace la protezione dei dati».

IV. **LA NUOVA DECISIONE QUADRO SULLA PROTEZIONE DEI DATI TRATTATI NELL'AMBITO DELLA COOPERAZIONE GIUDIZIARIA E DI POLIZIA IN MATERIA PENALE**

16. Il quadro giuridico applicabile in materia di protezione dei dati acquista importanza ancora maggiore in considerazione dell'intensificarsi degli scambi di dati personali tra le autorità giudiziarie previsto dalla comunicazione. In proposito, il GEPD rileva che, tre anni dopo la proposta iniziale della Commissione, il Consiglio dell'Unione europea ha adottato, il 27 novembre, la decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale ([8]). Questo nuovo atto legislativo fornirà un quadro giuridico generale in materia di protezione dei dati per le questioni del «terzo pilastro», in aggiunta alle disposizioni in materia di protezione dei dati del «primo pilastro» di cui alla direttiva 95/46/CE.

17. Il GEPD accoglie favorevolmente questo strumento giuridico come primo passo importante per la protezione dei dati nella cooperazione giudiziaria e di polizia. Tuttavia, il livello di protezione dei dati previsto nel testo finale non è pienamente soddisfacente. In particolare, la decisione quadro riguarda unicamente i dati giudiziari e di polizia scambiati tra Stati membri, autorità e sistemi dell'UE e non riguarda i dati a livello interno. Inoltre, la decisione quadro adottata non prevede l'obbligo di operare una distinzione tra le diverse categorie di persone interessate — quali indagati, criminali, testimoni e vittime — che garantirebbe un trattamento dei loro dati con garanzie più appropriate. Non è completamente in linea con la direttiva 95/46/CE, soprattutto per quanto riguarda la limitazione delle finalità per le quali i dati personali potrebbero essere sottoposti ad ulteriore trattamento. Non prevede neppure la creazione di un gruppo indipendente formato da autorità garanti della protezione dei dati nazionali e dell'UE che potrebbe assicurare sia un migliore coordinamento tra le autorità garanti sia un contributo sostanziale all'applicazione uniforme della decisione quadro.

18. Ciò implica che, in un contesto in cui si compiono molti sforzi per elaborare sistemi comuni di scambio transfrontaliero di dati personali, sussistono divergenze per quanto riguarda le norme in base alle quali tali dati sono trattati e i cittadini possono esercitare i loro diritti nei diversi paesi dell'UE.

19. Il GEPD ricorda ancora una volta che garantire un elevato livello di protezione dei dati in materia di cooperazione giudiziaria e di polizia nonché la conformità con la direttiva 95/46/CE costituisce una necessaria misura complementare ad altre misure introdotte o previste per agevolare gli scambi transfrontalieri di dati personali in ordine all'applicazione della legge. Ciò deriva non solo dal diritto dei cittadini al rispetto del diritto fondamentale di protezione dei dati personali, ma anche dalla necessità che le autorità preposte all'applicazione della legge assicurino la qualità dei dati scambiati — come conferma l'allegato della comunicazione per quanto riguarda l'interconnessione dei casellari giudiziari —, la fiducia fra le autorità dei vari paesi e, in ultima analisi, la validità giuridica delle prove raccolte in un contesto transfrontaliero.

20. Il GEPD incoraggia pertanto le istituzioni dell'UE a tenere specificamente conto di questi elementi non solo nell'attuazione delle misure previste nella comunicazione, ma anche nell'ottica di avviare quanto prima le riflessioni sugli ulteriori miglioramenti da apportare al quadro giuridico per la protezione dei dati in ordine all'applicazione della legge.

V. **PROGETTI DI GIUSTIZIA ELETTRONICA**

Strumenti di giustizia elettronica a livello europeo

21. Il GEPD riconosce che gli scambi di dati personali sono elementi essenziali nella creazione di uno spazio di sicurezza, libertà e giustizia. Per questo motivo il GEPD è

([8]) In attesa delle pubblicazione nella GU.

favorevole alla proposta di elaborare una strategia in materia di giustizia elettronica, pur sottolineando l'importanza che riveste la protezione dei dati in tale contesto. Infatti, il rispetto della protezione dei dati non è soltanto un obbligo legale ma anche un fattore determinante per il buon esito dei sistemi previsti, vale a dire assicurare la qualità degli scambi di dati. Questo vale anche per le istituzioni e gli organi quando trattano dati personali e quando elaborano nuove politiche. Norme e principi dovrebbero essere applicati e messi in pratica e dovrebbero essere presi in considerazione, in particolare, nelle fasi di progettazione e di allestimento dei sistemi d'informazione. La tutela della vita privata e la protezione dei dati sono in sostanza «fattori di successo cruciali» per una società dell'informazione prospera ed equilibrata. È pertanto importante investire in questo campo e farlo quanto più rapidamente possibile.

22. Al riguardo il GEPD sottolinea che la comunicazione non prevede la creazione di una banca dati centrale europea. Si compiace del fatto che siano preferite architetture decentrate. Il GEPD ricorda il suo parere sull'ECRIS ([9]) e sull'iniziativa di Prüm ([10]). Nel suo parere sull'ECRIS, il GEPD ha indicato che un'architettura decentrata evita di replicare ulteriormente i dati personali in una banca dati centrale. Nel suo parere sull'iniziativa di Prüm, ha raccomandato di tenere debitamente conto della dimensione del sistema nelle discussioni sull'interconnessione tra banche dati. In particolare, dovrebbero essere previsti formati specifici per la trasmissione dei dati, come le richieste di informazioni estratte dal casellario giudiziario, tenuto conto anche delle diversità linguistiche, e dovrebbe essere verificata costantemente l'accuratezza degli scambi dei dati. Si dovrebbe tener conto di questi elementi anche nell'ambito delle iniziative che deriveranno dalla strategia in materia di giustizia elettronica.

23. La Commissione europea intende contribuire al potenziamento e allo sviluppo degli strumenti di giustizia elettronica a livello europeo, in stretto coordinamento con gli Stati membri e gli altri partner coinvolti. Mentre sostiene gli sforzi degli Stati membri, essa intende sviluppare in prima persona un certo numero di strumenti informatici intesi a potenziare l'interoperabilità dei sistemi, agevolare l'accesso del pubblico alla giustizia e alla comunicazione fra autorità giudiziarie, nonché realizzare cospicue economie di scala a livello europeo. Quanto all'interoperabiltà del software utilizzato dagli Stati membri, non tutti gli Stati membri devono necessariamente utilizzare il medesimo software — anche se ciò sarebbe la soluzione più pratica — ma i software utilizzati devono essere pienamente interoperabili.

24. Il GEPD raccomanda che l'interconnessione e l'interoperabilità dei sistemi tengano debitamente conto del principio di limitazione delle finalità e si fondino sulle norme relative alla protezione dei dati («tutela della vita privata fin dalla progettazione», «*privacy by design*»). Qualsiasi forma di interazione tra due sistemi diversi dovrebbe essere documentata in modo esauriente. L'interoperabilità non dovrebbe mai condurre ad una situazione in cui un'autorità, non autorizzata ad accedere a taluni dati o ad utilizzarli, può ottenere tale accesso tramite un altro sistema di informazione. Il GEPD desidera ribadire il fatto che l'interoperabilità non dovrebbe di per sé giustificare la violazione del principio di limitazione delle finalità ([11]).

25. È inoltre essenziale assicurare che l'aumento dello scambio transfrontaliero di dati personali vada di pari passo con il rafforzamento del controllo e della cooperazione da parte delle autorità preposte alla protezione dei dati. Il GEPD ha già sottolineato, nel suo parere del 29 maggio 2006 sulla decisione quadro relativa agli scambi di informazioni estratte dal casellario giudiziario ([12]), che tale proposta non dovrebbe riguardare solo la cooperazione tra le autorità centrali, ma anche la cooperazione tra le varie autorità competenti per la protezione dei dati. Ciò è diventato ancor più importante in quanto i negoziati sulla decisione quadro relativa alla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia ([13]), recentemente adottata, hanno portato alla soppressione della disposizione che istituiva un gruppo che riunisce le autorità dell'UE per la protezione dei dati e ne coordina le attività con riguardo al trattamento dei dati nel quadro della cooperazione di polizia e giudiziaria in materia penale. Pertanto, onde garantire l'efficace controllo e la buona qualità della circolazione transfrontaliera dei dati estratti dal casellario giudiziario, sarebbe necessario predisporre meccanismi di effettivo coordinamento tra le autorità preposte alla protezione dei dati ([14]). Questi meccanismi dovrebbero tener conto anche della competenza in materia di controllo del GEPD per quanto riguarda l'infrastruttura S-TESTA ([15]). Gli strumenti di giustizia elettronica potrebbero sostenere tali meccanismi che potrebbero essere sviluppati in stretta cooperazione con le autorità preposte alla protezione dei dati.

26. Al punto 4.2.1 la comunicazione rileva l'importanza che gli scambi di informazioni estratte dal casellario giudiziario si estendano oltre la cooperazione giudiziaria e integrino altri obiettivi, ad es. controllare l'accesso a determinate professioni. Il GEPD sottolinea che qualsiasi trattamento di dati personali per fini diversi da quelli per i quali sono stati raccolti dovrebbe rispettare le condizioni specifiche stabilite dalla legislazione vigente in materia di protezione dei dati. In particolare, il trattamento dei dati personali per

([9]) Cfr. nota 4, punto 18.
([10]) GU C 89 del 10.4.2008, pag. 4.
([11]) GU C 91 del 19.4.2006, pag. 53. Cfr. anche le osservazioni del GEPD sulla comunicazione della Commissione sull'interoperabilità tra le banche dati europee, Bruxelles, 10.3.2006.
([12]) GU C 313 del 20.12.2006, pag. 26.
([13]) Cfr sopra, parte IV.
([14]) Cfr. il parere del GEPD sull'ECRIS, punti 8 e 37-38.
([15]) Al riguardo, cfr. punti 27-28 più avanti.

altre finalità dovrebbe essere autorizzato soltanto se necessario al perseguimento degli interessi contemplati dalla normativa comunitaria sulla protezione dei dati ([16]) e purché stabilito da disposizioni legislative.

27. La comunicazione afferma, riguardo all'interconnessione dei casellari giudiziari, che nell'ottica dell'entrata in vigore della decisione quadro sullo scambio delle informazioni estratte dal casellario giudiziario, la Commissione avvierà due studi di fattibilità per monitorare l'evoluzione del progetto e per estendere lo scambio delle informazioni ai cittadini degli Stati terzi oggetto di condanne penali. Nel 2009, la Commissione metterà a disposizione degli Stati membri un programma informatico che dovrà permettere lo scambio in tempi rapidi di tutti i casellari giudiziari. Questo sistema di riferimento, in combinazione con s-TESTA per lo scambio di informazioni, permetterà di realizzare economie di scala evitando ai singoli Stati membri di dover predisporre un proprio sistema e semplificherà il funzionamento tecnico del progetto.

28. In tale ottica, il GEPD è favorevole all'uso dell'infrastruttura s-TESTA, rivelatasi un sistema affidabile per lo scambio dei dati, e raccomanda che gli elementi statistici relativi ai sistemi previsti per lo scambio dei dati siano definiti con precisione, tenendo debitamente conto della necessità di assicurare il controllo della protezione dei dati. Ad esempio, i dati statistici potrebbero includere esplicitamente elementi come il numero di richieste di accesso o di rettifica dei dati personali, la durata e la completezza del processo di aggiornamento, la qualifica delle persone che possono accedere ai dati e i casi di violazione della sicurezza. Inoltre, i dati statistici e le relazioni basate su di essi dovrebbero essere messi integralmente a disposizione delle autorità competenti per la protezione dei dati.

Traduzione automatica e banca dati di traduttori

29. L'uso della traduzione automatica è uno strumento utile e potrebbe favorire la reciproca comprensione tra i soggetti competenti negli Stati membri. Tuttavia, l'uso della traduzione automatica non dovrebbe tradursi in una minore qualità delle informazioni scambiate, specie quando queste sono usate per adottare decisioni aventi effetti giuridici per le persone interessate. Il GEPD sottolinea l'importanza di definire e circoscrivere precisamente l'uso della traduzione automatica. L'uso della traduzione automatica per la trasmissione di informazioni che non sono state accuratamente pretradotte, come osservazioni o precisazioni supplementari aggiunte in casi specifici, rischia di compromettere la qualità delle informazioni trasmesse — e pertanto delle decisioni prese basandosi su tali informazioni — e dovrebbe quindi essere esclusa in linea di principio ([17]). Il GEPD suggerisce di tener conto di questa raccomandazione nelle disposizioni che deriveranno dalla comunicazione.

30. La comunicazione vuole creare una banca dati di traduttori e interpreti giudiziari che consenta di migliorare la qualità della traduzione e dell'interpretariato in ambito giudiziario. Il GEPD aderisce a questo proposito ma ricorda che la banca dati sarà soggetta all'applicazione della pertinente normativa sulla protezione dei dati. In particolare, se la banca dati dovesse contenere dati relativi a valutazioni del lavoro svolto dai traduttori, potrebbe essere soggetta al controllo preventivo delle autorità competenti per la protezione dei dati.

Verso un piano d'azione europeo in materia di giustizia elettronica

31. Al punto 5 della comunicazione, si afferma che è necessario procedere a una chiara ripartizione delle responsabilità fra la Commissione, gli Stati membri e gli altri soggetti della cooperazione giudiziaria. La Commissione assumerà un ruolo generale di coordinamento, favorendo gli scambi di buone pratiche e lavorerà all'ideazione e all'allestimento del portale «Giustizia elettronica», coordinando le informazioni che vi figurano. Inoltre, la Commissione proseguirà i lavori sull'interconnessione dei casellari giudiziari e continuerà ad assumersi la responsabilità diretta della rete giudiziaria civile e a sostenere la rete giudiziaria penale. Gli Stati membri dovranno aggiornare le informazioni relative ai rispettivi sistemi giuridici nel sito in materia di giustizia elettronica. Altri soggetti coinvolti sono le reti giudiziarie in materia civile e penale ed Eurojust. Essi svilupperanno, a stretto contatto con la Commissione, gli strumenti necessari a una operazione giudiziaria più efficiente, in particolare gli strumenti di traduzione automatica e i dispositivi di sicurezza del sistema di scambio. La comunicazione contiene in allegato una proposta di piano d'azione e di calendario per i vari progetti.

32. In questo contesto, il GEPD sottolinea che nel sistema ECRIS, da un lato, non è creata alcuna banca dati centrale europea e non è previsto un accesso diretto a banche dati come quelle che contengono casellari giudiziari di altri Stati membri, mentre, dall'altro, a livello nazionale la responsabilità di fornire informazioni corrette è centralizzata presso le autorità centrali degli Stati membri. Nell'ambito di questo meccanismo gli Stati membri sono responsabili della gestione delle banche dati nazionali nonché del funzionamento efficace degli scambi. Non è chiaro se siano o no responsabili del software di interconnessione. La Commissione metterà a disposizione degli Stati membri un programma informatico che dovrà permettere lo scambio in tempi rapidi di tutti i casellari giudiziari. Questo sistema di riferimento sarà usato in combinazione con s-TESTA per lo scambio di informazioni.

33. Il GEPD presume che simili sistemi potrebbero essere applicati anche nell'ambito di iniziative analoghe in materia

([16]) Cfr. in particolare l'articolo 13 della direttiva 95/46 e l'articolo 20 del regolamento 45/2001.

([17]) Cfr. il parere del GEPD sull'ECRIS, punti 39-40.

di giustizia elettronica e che la Commissione sarà responsabile dell'infrastruttura comune, sebbene questo non sia precisato nella comunicazione. Il GEPD suggerisce, per motivi di certezza giuridica, di chiarire questa responsabilità nelle disposizioni che deriveranno dalla comunicazione.

Progetti di giustizia elettronica

34. In allegato figurano alcuni progetti da svolgere nel corso dei prossimi cinque anni. Il primo progetto sullo sviluppo delle pagine giustizia elettronica riguarda il portale «Giustizia elettronica». L'azione da avviare consiste in uno studio di fattibilità e di allestimento del portale. Sono previste inoltre la messa a punto dei metodi di gestione e la messa in linea di informazioni in tutte le lingue dell'UE. Il secondo e il terzo progetto riguardano l'interconnessione dei casellari giudiziari. Il progetto 2 interessa l'interconnessione dei casellari giudiziari nazionali, mentre il progetto 3 prevede la creazione di un indice europeo dei cittadini di paesi terzi condannati, oltre a uno studio di fattibilità e alla presentazione di una proposta legislativa. Il GEPD osserva che quest'ultimo progetto non figura più nel programma di lavoro della Commissione e si chiede se ciò stia ad indicare una modifica dei progetti previsti dalla Commissione o il mero rinvio di tale progetto specifico.

35. La comunicazione riporta inoltre tre progetti nel settore degli scambi elettronici e tre in materia di ausilio alla traduzione. Sarà avviato un progetto pilota che prevede la graduale creazione di un vocabolario giuridico multilingue comparato. Altri progetti importanti riguardano la creazione di moduli dinamici che accompagnino i testi legislativi europei e la promozione dell'uso delle videoconferenze da parte delle autorità giudiziarie. Infine, nel quadro del forum giustizia elettronica, saranno organizzate riunioni annuali attorno a tematiche relative alla giustizia elettronica e sarà impartita agli operatori di giustizia una formazione nel settore della cooperazione giudiziaria. Il GEPD propone che per tali riunioni e formazioni sia prestata sufficiente attenzione alle leggi e alle prassi in materia di protezione dei dati.

36. L'allegato prevede pertanto un'ampia gamma di strumenti europei destinati a facilitare lo scambio di informazioni tra attori nei vari Stati membri. Fra questi strumenti un ruolo importante svolgerà il portale «Giustizia elettronica», la cui responsabilità incomberà principalmente alla Commissione.

37. Una caratteristica comune a molti di questi strumenti consiste nel fatto che le informazioni e i dati personali saranno scambiati e gestiti, sia a livello nazionale che di UE, da vari attori soggetti agli obblighi in materia di protezione dei dati e alle autorità di controllo di cui alla direttiva 95/46/CE e al regolamento (CE) n. 45/2001. A tale riguardo, come ha già chiarito il GEPD nel suo parere sul sistema di informazione del mercato interno (IMI) [18], è essenziale garantire le responsabilità inerenti al rispetto delle norme in materia di protezione dei dati siano esercitate in modo efficace e continuo.

38. Ciò presuppone fondamentalmente, da un lato, una chiara definizione e attribuzione delle responsabilità in materia di trattamento dei dati nel quadro di tali sistemi, dall'altro, l'eventuale definizione di adeguati meccanismi di coordinamento, in particolare per quanto riguarda il controllo.

39. Il ricorso alle nuove tecnologie rappresenta uno dei capisaldi delle iniziative in materia di giustizia elettronica: l'interconnessione dei registri nazionali, lo sviluppo della firma elettronica, le reti sicure, le piattaforme di scambio virtuale e il ricorso più frequente alle videoconferenze costituiranno negli anni a venire altrettanti elementi essenziali delle iniziative in materia di giustizia elettronica.

40. In tale contesto, è essenziale che gli aspetti relativi alla protezione dei dati siano presi in considerazione in una fase quanto più precoce possibile e incorporati nell'architettura degli strumenti previsti. In particolare, speciale importanza rivestono sia l'architettura del sistema che l'attuazione di adeguate misure di sicurezza. Grazie all'approccio «*privacy by design*», le pertinenti iniziative in materia di giustizia elettronica dovrebbero permettere una gestione efficace dei dati personali, rispettando nel contempo i principi di protezione dei dati e la sicurezza degli scambi degli stessi tra diverse autorità.

41. Inoltre, il GEPD rileva che gli strumenti tecnologici dovrebbero essere utilizzati non solo per garantire lo scambio di informazioni, ma anche per rafforzare i diritti degli interessati. In tale ottica, il GEPD si rallegra che la comunicazione preveda la possibilità per i cittadini di ottenere il proprio casellario giudiziario in linea e nella lingua di loro scelta [19]. A tale proposito, il GEPD ricorda che, nel suo parere sulla proposta della Commissione relativa allo scambio di informazioni estratte dal casellario giudiziario, si era rallegrato della possibilità che gli interessati potessero chiedere informazioni sul proprio casellario giudiziario all'autorità centrale di uno Stato membro, a condizione di essere o di essere stati residenti o cittadini dello Stato membro richiesto o dello Stato membro richiedente. Il GEPD ha altresì proposto, nell'ambito del coordinamento dei sistemi di sicurezza sociale, di utilizzare come «sportello unico» l'autorità più vicina all'interessato. Pertanto, il GEPD

[18] GU C 270 del 25.10.2008, pag. 1.
[19] Ved. comunicazione, pag. 6.

incoraggia la Commissione a proseguire nella stessa direzione, promuovendo gli strumenti tecnologici — segnatamente in materia di accesso in linea — per consentire ai cittadini di controllare meglio i loro dati personali anche quando si spostano da uno Stato membro all'altro.

VI. **CONCLUSIONI**

42. Il GEPD appoggia l'attuale proposta di istituzione della giustizia elettronica e raccomanda di tenere conto delle osservazioni formulate nel presente parere, segnatamente delle seguenti:

— tenere conto della recente decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale — compresi i punti deboli — non solo nell'attuazione delle misure previste nella comunicazione, ma anche nell'ottica di avviare quanto prima le riflessioni sugli ulteriori miglioramenti da apportare al quadro giuridico per la protezione dei dati nell'applicazione della legge;

— includere procedure amministrative nella giustizia elettronica. Nell'ambito di tale nuovo elemento, si dovrebbero avviare progetti di giustizia elettronica intesi a rafforzare la visibilità delle norme sulla protezione dei dati e delle autorità nazionali preposte alla protezione dei dati, segnatamente in relazione ai tipi di dati trattati nel quadro dei progetti stessi;

— continuare a privilegiare le architetture decentrate;

— far sì che l'interconnessione e l'interoperabilità dei sistemi tengano debitamente conto del principio di limitazione delle finalità;

— assegnare chiare responsabilità a tutti gli attori che trattano dati personali nel quadro dei sistemi previsti e prevedere meccanismi di efficace coordinamento tra le autorità incaricate della protezione dei dati;

— far sì che il trattamento di dati personali per fini diversi da quelli per i quali sono stati raccolti debba rispettare le condizioni specifiche fissate nella legislazione applicabile in materia di protezione dei dati;

— definire e circoscrivere chiaramente l'uso della traduzione automatica, al fine di favorire la reciproca comprensione dei vari reati penali senza rischiare di compromettere la qualità delle informazioni trasmesse;

— chiarire la responsabilità della Commissione relativa alle infrastrutture comuni, quale l's-TESTA;

— per quanto riguarda l'uso delle nuove tecnologie, far sì che gli aspetti relativi alla protezione dei dati siano presi in considerazione in una fase quanto più precoce possibile («*privacy by design*») e promuovere gli strumenti tecnologici per consentire ai cittadini di controllare meglio i loro dati personali anche quando si spostano da uno Stato membro all'altro.

Fatto a Bruxelles, il 19 dicembre 2008.

Peter HUSTINX

garante europeo della protezione dei dati

Progetto di parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera

(2009/C 128/03)

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,

vista la richiesta di parere a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 spedita al GEPD il 2 luglio 2008,

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE

La proposta di direttiva concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera

1. Il 2 luglio 2008 la Commissione ha adottato una proposta di direttiva del Parlamento europeo e del Consiglio concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (in seguito denominata «la proposta») ([1]). La proposta è stata trasmessa dalla Commissione al GEPD per consultazione, a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001.

2. La proposta mira a istituire un quadro comunitario per la prestazione di assistenza sanitaria transfrontaliera all'interno dell'UE laddove l'assistenza di cui i pazienti hanno bisogno venga prestata in uno Stato membro diverso dal loro paese di origine. Il quadro si articola in tre settori principali:

— la definizione di principi comuni a tutti i sistemi sanitari dell'UE, che precisino chiaramente le competenze degli Stati membri;

— lo sviluppo di un quadro specifico per l'assistenza sanitaria transfrontaliera, che indichi chiaramente i diritti dei pazienti di ricevere assistenza sanitaria in un altro Stato membro;

— la promozione della cooperazione UE nell'assistenza sanitaria, in settori quali il riconoscimento delle prescrizioni rilasciate in altri paesi, le reti di riferimento europee, la valutazione delle tecnologie sanitarie, la raccolta dei dati, la qualità e la sicurezza.

3. Il quadro ha un duplice obiettivo: garantire sufficiente chiarezza in merito ai diritti al rimborso spettanti per l'assistenza sanitaria prestata in altri Stati membri e garantire che i necessari requisiti di qualità, sicurezza ed efficienza dell'assistenza sanitaria siano soddisfatti anche quando si tratta di assistenza transfrontaliera.

4. L'attuazione di un sistema di assistenza sanitaria transfrontaliera richiede lo scambio dei pertinenti dati personali relativi alla salute (in seguito denominati «dati sanitari») dei pazienti tra le organizzazioni e gli operatori sanitari autorizzati dei diversi Stati membri. Tali dati sono considerati sensibili e sono soggetti alle norme di protezione dei dati più rigorose di cui all'articolo 8 della direttiva 95/45/CE riguardante categorie particolari di dati.

Consultazione del GEPD

5. Il GEPD accoglie con soddisfazione il fatto di essere stato consultato sulla questione e il riferimento a tale consultazione figurante nel preambolo della proposta, in conformità dell'articolo 28 del regolamento (CE) n. 45/2001.

6. È la prima volta che il GEPD viene formalmente consultato su una proposta di direttiva nel settore dell'assistenza sanitaria. Pertanto nel presente parere alcune delle osservazioni sono di più ampia portata e riguardano questioni generali della protezione dei dati personali nel settore dell'assistenza sanitaria, che potrebbero applicarsi anche ad altri strumenti giuridici pertinenti (vincolanti o no).

([1]) COM(2008) 414 definitivo Si noti che nella stessa data è stata adottata anche una comunicazione complementare della Commissione intitolata «Quadro comunitario concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera» (COM(2008) 415 definitivo). Tuttavia, poiché la comunicazione ha soltanto carattere piuttosto generale, il GEPD ha scelto di concentrarsi sulla proposta di direttiva.

7. Il GEPD desidera anzitutto esprimere sostegno alle iniziative volte a migliorare le condizioni dell'assistenza sanitaria transfrontaliera. Questa proposta andrebbe in effetti collocata nel contesto del programma comunitario globale di miglioramento della salute dei cittadini nella società dell'informazione. Altre iniziative in tal senso sono la direttiva e la comunicazione, previste dalla Commissione, sulla donazione e il trapianto di organi ([1]), la raccomandazione sull'interoperabilità dei sistemi di cartelle cliniche elettroniche ([2]) e la comunicazione prevista sulla telemedicina ([3]). Il GEPD è tuttavia preoccupato dal fatto che tutte queste iniziative correlate non siano strettamente collegate e/o interconnesse nel settore della tutela della vita privata e della sicurezza dei dati, ostacolando in tal modo l'adozione di un approccio uniforme alla protezione dei dati nell'assistenza sanitaria, soprattutto per quanto riguarda l'uso delle nuove tecnologie dell'informazione e della comunicazione. Ad esempio, benché l'attuale proposta di direttiva menzioni esplicitamente la telemedicina al considerando 10, non viene fatto alcun riferimento all'aspetto di protezione dei dati della pertinente comunicazione della Commissione. Inoltre, nonostante le cartelle cliniche elettroniche siano un possibile modo di comunicazione transfrontaliera di dati sanitari, non si fa alcun riferimento alle questioni inerenti alla vita privata trattate nella pertinente raccomandazione della Commissione ([4]). Questo dà l'impressione che una prospettiva globale di tutela della vita privata nell'assistenza sanitaria non sia ancora chiaramente definita e, in alcuni casi, manchi completamente.

8. Lo si può riscontrare chiaramente anche nell'attuale proposta, nella quale il GEPD constata con rammarico che le implicazioni in relazione alla protezione dei dati non sono trattate in termini concreti. Ci sono ovviamente riferimenti alla protezione dei dati, ma essi sono soprattutto di carattere generale e non rispecchiano adeguatamente le esigenze e i requisiti dell'assistenza sanitaria transfrontaliera per quanto concerne la tutela della vita privata.

9. Il GEPD desidera sottolineare che un approccio uniforme e solido alla protezione dei dati nell'insieme degli strumenti proposti in materia di assistenza sanitaria non solo garantirà il diritto fondamentale dei cittadini alla protezione dei loro dati ma contribuirà anche all'ulteriore sviluppo dell'assistenza sanitaria transfrontaliera nell'UE.

II. LA PROTEZIONE DEI DATI NELL'ASSISTENZA SANITARIA TRANSFRONTALIERA

Contesto generale

10. Lo scopo di maggior rilievo della Comunità europea è stato quello di istituire un mercato interno, uno spazio senza frontiere interne nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali. Consentire ai cittadini di circolare e risiedere più facilmente in Stati membri diversi da quello di origine ha evidentemente posto questioni in relazione all'assistenza sanitaria. Per tale motivo, negli anni novanta, la Corte di giustizia ha trattato, nel contesto del mercato interno, questioni relative al possibile rimborso di spese mediche sostenute in un altro Stato membro. La Corte di giustizia ha riconosciuto che la libera prestazione di servizi, prevista all'articolo 49 del trattato CE, include la libertà per le persone di recarsi in un altro Stato membro per fruire di cure mediche ([5]). Di conseguenza i pazienti che desideravano ricevere un'assistenza sanitaria transfrontaliera non potevano più essere trattati in modo diverso dai cittadini del proprio paese di origine che fruivano delle stesse cure mediche senza attraversare la frontiera.

11. Tali sentenze della Corte sono al centro dell'attuale proposta. Poiché la giurisprudenza della Corte è basata su singoli casi, l'attuale proposta intende fare maggiore chiarezza per garantire un'applicazione più generale ed efficace delle libertà inerenti alla fruizione e alla prestazione dei servizi sanitari. Tuttavia, come già indicato, la proposta fa anche parte di un programma più ambizioso che mira al miglioramento della salute dei cittadini nella società dell'informazione, che secondo l'UE offre grandi possibilità di miglioramento dell'assistenza sanitaria transfrontaliera mediante il ricorso alle tecnologie dell'informazione.

12. Per ovvi motivi, la definizione di norme sull'assistenza sanitaria transfrontaliera è una questione delicata. Tocca un settore sensibile in cui gli Stati membri hanno istituito sistemi nazionali divergenti, ad esempio per quanto riguarda l'assicurazione e il rimborso dei costi o l'organizzazione dell'infrastruttura dell'assistenza sanitaria, incluse le applicazioni e le reti d'informazione in materia di assistenza sanitaria. Anche se nell'attuale proposta il legislatore comunitario si concentra unicamente sull'assistenza sanitaria transfrontaliera, le norme influenzeranno quantomeno il modo in cui sono organizzati i sistemi nazionali di assistenza sanitaria.

13. Il miglioramento delle condizioni dell'assistenza sanitaria transfrontaliera andrà a vantaggio dei cittadini, comportando tuttavia nel contempo alcuni rischi per gli stessi. Occorre risolvere molti problemi pratici insiti nella cooperazione transfrontaliera tra persone di diversi paesi che parlano lingue diverse. Poiché la salute riveste la massima importanza per ogni cittadino, dovrebbe essere escluso qualsiasi rischio di cattiva comunicazione e di conseguente errore. Va da sé che l'accrescimento dell'assistenza sanitaria transfrontaliera unito al ricorso alle tecnologie dell'informazione più recenti ha forti implicazioni sulla protezione dei dati personali. Uno scambio più efficiente e quindi crescente di dati sanitari, la distanza sempre più grande tra

([1]) Annunciate nel programma di lavoro della Commissione.
([2]) Raccomandazione della Commissione, del 2 luglio 2008, sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche (notificata con il numero C(2008) 3282), GU L 190 del 18.7.2008, pag. 37.
([3]) Annunciata nel programma di lavoro della Commissione.
([4]) Al riguardo è rivelatore il fatto che nessun riferimento alla tutela della vita privata e alla protezione dei dati figuri nella comunicazione di cui alla nota 1, che intende stabilire un quadro comunitario concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera.
([5]) Cfr causa 158/96, *Kohll*, racc. [1998], pag. I-1931, punto 34. Cfr tra l'altro anche causa C-157/99, *Smits e Peerbooms*, racc. [2001], pag. I-5473 e causa C-385/99, *Müller-Fauré e Van Riet*, racc. [2003], pag. I-12403.

persone e organismi interessati e la diversità delle normative nazionali di attuazione delle norme sulla protezione dei dati pongono questioni di sicurezza dei dati e di certezza del diritto.

Protezione dei dati sanitari

14. È necessario sottolineare che i dati sanitari sono considerati una categoria speciale di dati che merita un livello di protezione più elevato. Come affermato di recente dalla Corte europea dei diritti dell'uomo nel contesto dell'articolo 8 della Convenzione europea dei diritti dell'uomo: la protezione dei dati personali, in particolare dei dati medici, è di importanza fondamentale per l'esercizio da parte di una persona del diritto al rispetto della sua vita privata e familiare, garantito dall'articolo 8 della convenzione ([1]). Prima di passare alla spiegazione delle norme più rigorose relative al trattamento dei dati sanitari di cui alla direttiva 95/46/CE, in appresso figura un breve esame della nozione di «dati sanitari».

15. La direttiva 95/46/CE non riporta una definizione esplicita di dati sanitari. Generalmente se ne dà un'interpretazione ampia, che spesso definisce i dati sanitari come dati personali che hanno un legame esplicito e stretto con la descrizione dello stato di salute di una persona ([2]). Al riguardo i dati sanitari includono normalmente i dati medici (ad es. impegnative e prescrizioni del medico, referti medici, esami di laboratorio, radiografie, ecc.) e i dati finanziari e amministrativi concernenti la salute (ad es. documenti relativi ai ricoveri ospedalieri, numero di sicurezza sociale, calendario delle consultazioni mediche, fatture delle prestazioni di servizi di assistenza sanitaria, ecc.). Va rilevato che i termini «dati medici» ([3]) sono a volte usati per indicare dati concernenti la salute, come pure i termini «dati relativi all'assistenza sanitaria» ([4]). Nel presente parere saranno sistematicamente utilizzati i termini «dati sanitari».

16. La norma ISO 27799 fornisce un'utile definizione dei termini «dati sanitari», intesi come qualsiasi informazione attinente alla salute fisica o mentale di un soggetto, o alla prestazione di un servizio sanitario a tale soggetto e che può includere: a) informazioni sulla registrazione del soggetto ai fini della prestazione di servizi sanitari; b) informazioni sui pagamenti o l'ammissibilità all'assistenza sanitaria riguardo al soggetto; c) un numero, simbolo o elemento specifico attribuito ad un soggetto per identificarlo in modo univoco a fini sanitari; d) qualsiasi informazione sul soggetto raccolta nel corso della prestazione di servizi sanitari allo stesso; e) informazioni derivanti da prove od esami effettuati su una parte del corpo o una sua sostanza; e f) l'identificazione di una persona (operatore sanitario) come fornitore dell'assistenza sanitaria ad un soggetto.

17. Il GEPD è decisamente favorevole all'adozione di una definizione specifica per i termini «dati sanitari» nel contesto dell'attuale proposta, che potrebbe essere altresì utilizzata in futuro nell'ambito di altri testi pertinenti nella legislazione comunitaria (ved. sezione III in appresso).

18. L'articolo 8 della direttiva 95/46/CE stabilisce le norme sui trattamenti riguardanti categorie particolari di dati. Tali norme sono più rigorose rispetto a quelle relative al trattamento di altri dati, che figurano all'articolo 7 della direttiva 95/46/CE. L'articolo 8, paragrafo 1 stabilisce infatti esplicitamente che gli Stati membri *vietano*, tra l'altro, il trattamento di dati relativi alla salute. Nei successivi paragrafi del medesimo articolo sono elencate varie deroghe a tale divieto, ma queste sono più limitate rispetto ai motivi che giustificano il trattamento dei dati normali che figurano all'articolo 7. Ad esempio, il divieto non si applica qualora la persona interessata abbia dato il proprio consenso *esplicito* (articolo 8, paragrafo 2, lettera a)), che si contrappone al requisito della manifestazione di un consenso *inequivocabile* di cui all'articolo 7, lettera a) della direttiva 95/46/CE. La legislazione dello Stato membro può inoltre prevedere che in taluni casi anche il consenso della persona interessata non sia sufficiente per derogare al divieto. Il paragrafo 3 dell'articolo 8 è interamente dedicato al trattamento dei dati di carattere sanitario. Ai sensi di tale paragrafo il divieto di cui al paragrafo 1 non si applica quando il trattamento dei dati è necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure o alla gestione di centri di cura e quando il trattamento dei medesimi dati viene effettuato da un professionista in campo sanitario soggetto al segreto professionale sancito dalla legislazione nazionale, comprese le norme stabilite dagli organi nazionali competenti, o da un'altra persona egualmente soggetta a un obbligo di segreto equivalente.

19. L'articolo 8 della direttiva 95/46/CE pone un accento particolare sulla necessità che gli Stati membri forniscano garanzie appropriate o adeguate. Ad esempio, l'articolo 8, paragrafo 4 autorizza gli Stati membri a stabilire ulteriori deroghe al divieto di trattamento dei dati di natura delicata per motivi di interesse pubblico rilevante, purché siano previste le opportune garanzie. In termini generali, ciò sottolinea la responsabilità degli Stati membri di prestare un'attenzione particolare al trattamento dei dati di natura delicata, come quelli relativi alla salute.

Protezione dei dati sanitari nelle situazioni transfrontaliere

Responsabilità condivise tra Stati membri

20. Gli Stati membri dovrebbero essere particolarmente consapevoli delle responsabilità succitate allorché si pone la questione dello scambio transfrontaliero di dati sanitari. Come

([1]) Cfr. CEDU 17 luglio 2008, *I c. Finlandia* (ric. 20511/03), punto 38.
([2]) Cfr. Gruppo dell'articolo 29, documento di lavoro sul trattamento di dati personali relativi alla salute nelle cartelle cliniche elettroniche (EHR), febbraio 2007, WP 131, punto II.2. Cfr. anche sul senso ampio di dati personali: Gruppo dell'articolo 29, parere 4/2007 sul concetto di dati personali, WP 136.
([3]) Raccomandazione n. R(97)5 del Consiglio d'Europa sulla protezione dei dati medici.
([4]) ISO 27799:2008 «Informatica sanitaria — Gestione della sicurezza delle informazioni nella sanità utilizzando la ISO/IEC 27002».

rilevato in precedenza, lo scambio transfrontaliero di dati sanitari aumenta il rischio di imprecisione e di illegittimità nel trattamento dei dati. Ovviamente ciò può comportare conseguenze estremamente negative per la persona interessata. Sia lo Stato membro di affiliazione (dove il paziente è assicurato) sia lo Stato membro di cura (dove l'assistenza sanitaria transfrontaliera è effettivamente fornita) sono coinvolti in tale processo e pertanto sono entrambi responsabili.

21. In tale contesto, la sicurezza dei dati sanitari è una questione importante. Nella recente causa menzionata in precedenza la Corte europea dei diritti dell'uomo ha attribuito particolare rilievo alla riservatezza dei dati sanitari, affermando che il rispetto della riservatezza dei dati sanitari è un principio vitale dei sistemi giuridici di tutte le parti contraenti della convenzione. È di importanza cruciale non soltanto tutelare la vita privata di un paziente, ma anche conservare la sua fiducia nella professione medica e nei servizi sanitari in generale. ([1])

22. Le norme sulla protezione dei dati stabilite dalla direttiva 95/46/CE prevedono inoltre che lo Stato membro di affiliazione fornisca al paziente informazioni adeguate, corrette ed aggiornate riguardo al trasferimento dei suoi dati personali verso un altro Stato membro, ed inoltre garantisca il trasferimento sicuro dei dati verso detto Stato membro. Lo Stato membro di cura dovrebbe inoltre garantire il ricevimento sicuro di tali dati e fornire il livello appropriato di protezione al momento del trattamento effettivo dei dati stessi, conformemente alla propria legislazione nazionale in materia di protezione dei dati.

23. Il GEPD desidera chiarire all'interno della proposta le responsabilità condivise tra gli Stati membri, tenendo conto anche della comunicazione elettronica dei dati, in particolare nel contesto delle nuove applicazioni TIC, come illustrato in appresso.

Comunicazione elettronica dei dati sanitari

24. Lo scambio transfrontaliero di dati sanitari può essere migliorato principalmente mediante il ricorso alle tecnologie dell'informazione. Sebbene lo scambio di dati in un sistema di assistenza sanitaria transfrontaliera possa ancora avvenire per via cartacea (ad esempio il paziente si trasferisce in un altro Stato membro portando con sé tutti i propri dati sanitari pertinenti, come analisi di laboratorio, impegnative mediche, ecc.) si riscontra la chiara intenzione di ricorrere piuttosto a strumenti elettronici. La comunicazione elettronica dei dati sanitari sarà supportata da sistemi informatici in materia di assistenza sanitaria istituiti (o da istituire) negli Stati membri (in ospedali, cliniche, ecc.) nonché dall'utilizzo di nuove tecnologie, quali le applicazioni relative alle cartelle cliniche elettroniche (possibilmente operanti tramite internet), nonché altri strumenti quali le tessere sanitarie dei pazienti e dei medici. Ovviamente è anche possibile ricorrere a forme combinate di scambi cartacei ed elettronici, a seconda dei sistemi di assistenza sanitaria degli Stati membri.

25. Le applicazioni relative alla sanità elettronica (e-health) e alla telemedicina, che rientrano nell'ambito della direttiva proposta, dipenderanno esclusivamente dallo scambio di dati sanitari elettronici (ad esempio segni vitali, immagini, ecc.) abitualmente associati ad altri sistemi elettronici di informazione in materia di assistenza sanitaria già in uso negli Stati membri di cura e di affiliazione. Ciò include i sistemi operanti sulla base delle comunicazioni paziente-medico (ad esempio, il monitoraggio e la diagnosi a distanza) sia medico-medico (ad es. teleconsultazione tra operatori sanitari a fini di consulenza su casi specifici di assistenza sanitaria). Altre applicazioni specifiche di assistenza sanitaria nel quadro generale della prestazione di assistenza sanitaria transfrontaliera possono anche dipendere esclusivamente dallo scambio elettronico di dati, ad esempio nel caso delle prescrizioni elettroniche o delle impegnative elettroniche, già utilizzate a livello nazionale in alcuni Stati membri ([2]).

Problematiche in materia di scambio transfrontaliero di dati sanitari

26. Tenuto conto delle considerazioni succitate, nonché delle differenze tra i sistemi sanitari esistenti negli Stati membri e del continuo sviluppo delle applicazioni in materia di sanità elettronica, emergono due ordini di problematiche per quanto riguarda la protezione dei dati personali nell'assistenza sanitaria transfrontaliera: a) i diversi livelli di sicurezza che possono essere applicati dagli Stati membri per la protezione dei dati personali (in termini di misure tecniche e organizzative) e b) l'integrazione dei requisiti di tutela della vita privata nelle applicazioni in materia di sanità elettronica, in particolare per quanto riguarda i nuovi sviluppi. Occorre inoltre riservare un'attenzione particolare ad altri aspetti, quali l'uso secondario dei dati sanitari, in particolare nel settore della produzione di statistiche. Tali questioni sono analizzate nel resto della presente sezione.

Sicurezza dei dati negli Stati membri

27. Sebbene le direttive 95/46/CE e 2002/58/CE siano applicate in modo uniforme in Europa, l'interpretazione e l'attuazione di taluni elementi possono essere diverse a seconda dei paesi, specialmente in settori dove le disposizioni giuridiche sono generali e lasciate alla discrezione degli Stati membri. In questo contesto, il principale settore da analizzare è quello della sicurezza del trattamento, ossia delle misure (tecniche e organizzative) adottate dagli Stati membri per garantire la sicurezza dei dati sanitari.

([1]) CEDU 17 luglio 2008, *I c. Finlandia* (ric. 20511/03), punto 38.

([2]) Relazione eHealth ERA intitolata «Towards the Establishment of a European eHealth Research Area» (Verso l'istituzione di uno Spazio europeo della ricerca in materia di sanità elettronica), Commissione europea, Società dell'informazione e media, marzo 2007, http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf

28. Sebbene la protezione rigorosa dei dati sanitari rientri tra le responsabilità di tutti gli Stati membri, non esiste al momento una definizione comunemente accettata di livello di sicurezza «appropriato» per l'assistenza sanitaria all'interno dell'UE che possa essere applicato nel caso dell'assistenza sanitaria transfrontaliera. Pertanto, ad esempio, un ospedale in uno Stato membro può essere obbligato dalla normativa sulla protezione dei dati applicata a livello nazionale ad adottare misure di sicurezza specifiche (ad esempio, la definizione di una politica e di codici di condotta in materia di sicurezza, norme specifiche per l'esternalizzazione ed il ricorso a contraenti esterni, requisiti in materia di revisione dei conti, ecc.) mentre in altri Stati membri questo non avviene. Tali discrepanze possono avere delle conseguenze sullo scambio di dati transfrontaliero, specialmente nel caso degli scambi in forma elettronica, poiché non si può garantire che i dati siano protetti (sul piano tecnico e organizzativo) allo stesso livello nei diversi Stati membri.

29. Vi è quindi la necessità di un'ulteriore armonizzazione in questo settore, in termini di definizione di un insieme comune di requisiti di sicurezza in materia di assistenza sanitaria che i fornitori di servizi di assistenza sanitaria degli Stati membri dovrebbero comunemente adottare. Questa necessità è indubbiamente in linea con l'esigenza generale, evidenziata nella proposta, di definire principi comuni nell'ambito dei sistemi sanitari dell'UE.

30. A tal fine si dovrebbe intervenire in modo generico, senza imporre agli Stati membri soluzioni tecniche specifiche ma ponendo comunque le basi per il riconoscimento e l'accettazione reciproci, per es. in campi quali la definizione di una politica in materia di sicurezza, l'identificazione e l'autenticazione dei pazienti e del personale sanitario, ecc. Le attuali norme internazionali ed europee (per es. ISO e CEN) in materia di assistenza sanitaria e di sicurezza, così come concetti tecnici generalmente accettati e aventi fondamento giuridico (per es. le firme elettroniche [1]) potrebbero servire da tabella di marcia in questo tentativo.

31. Il GEPD è favorevole all'idea di armonizzare la sicurezza in materia di assistenza sanitaria a livello dell'UE e ritiene che la Commissione debba prendere iniziative al riguardo, già nel quadro della proposta in esame (si veda la sezione III *infra*).

Tutela della vita privata nelle applicazioni di sanità elettronica (*e-health*)

32. La tutela della vita privata e la sicurezza dovrebbero costituire parte integrante della progettazione e della realizzazione dei sistemi di assistenza sanitaria, in particolare delle applicazioni di sanità elettronica (*e-health*) menzionate nella proposta in esame (principio della «tutela della vita privata fin dalla progettazione», «*privacy by design*»). Questo indiscutibile requisito è già stato sostenuto in altri documenti orientativi pertinenti [2], sia di tipo generale, sia specificamente dedicati all'assistenza sanitaria [3].

33. Nel quadro dell'interoperabilità della sanità elettronica (*e-health*) discussa nella proposta, sarebbe opportuno sottolineare ancora una volta la nozione di «tutela della vita privata fin dalla progettazione» come base per ogni sviluppo prospettato. Questo concetto si applica a vari livelli: organizzativo, semantico, tecnico.

— A livello organizzativo, si dovrebbe tenere conto della tutela della vita privata nel definire le procedure necessarie per lo scambio di dati sanitari tra gli organismi di assistenza sanitaria degli Stati membri. Ciò può incidere direttamente sul tipo di scambio e sull'entità del trasferimento dei dati (per es. uso, ove possibile, di numeri di identificazione invece dei nomi dei pazienti).

— A livello semantico, i requisiti in materia di tutela della vita privata e di sicurezza dovrebbero essere integrati nelle nuove norme e nei nuovi programmi, per es. nella definizione del modello di prescrizione elettronica discusso nella proposta. A tal fine ci si potrebbe basare sulle norme tecniche esistenti in questo campo, per es. le norme in materia di riservatezza dei dati e di firma digitale, e si potrebbero affrontare le esigenze specifiche dell'assistenza sanitaria quali l'autenticazione, in base al ruolo, del personale sanitario qualificato.

— A livello tecnico, le architetture di sistema e le applicazioni destinate agli utenti dovrebbero adattare tecnologie di rafforzamento della tutela della vita privata, attuando la definizione semantica menzionata in precedenza.

34. Il GEPD ritiene che il campo delle prescrizioni elettroniche possa costituire il punto di partenza per l'integrazione dei requisiti in materia di tutela della vita privata e di sicurezza nella primissima fase di sviluppo (si veda la sezione III *infra*).

Altri aspetti

35. Un altro aspetto di cui si potrebbe tenere conto nel quadro dello scambio transfrontaliero di dati sanitari è l'uso secondario dei dati sanitari, in particolare l'uso dei dati a fini statistici, già previsto nella proposta attuale.

36. Come indicato in precedenza al punto 18, l'articolo 8, paragrafo 4 della direttiva 95/46 prevede la possibilità dell'uso secondario dei dati sanitari. Tuttavia, questo trattamento successivo dovrebbe essere effettuato solo per motivi «di interesse pubblico rilevante» e a condizione che siano previste «le opportune garanzie» sulla base della legislazione nazionale o di una decisione dell'autorità di controllo [4]. Inoltre, il trattamento di dati a fini statistici, come sostenuto anche nel parere del GEPD sulla proposta di regolamento relativo alle statistiche comunitarie sulla sanità

[1] Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche, GU L 13 del 19.1.2000, pag. 12-20.

[2] «The EDPS and EU Research and Technological Development», documento orientativo, GEPD, aprile 2008, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf

[3] Raccomandazione della Commissione, del 2 luglio 2008, sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche [notificata con il numero C(2008) 3282], GU L 190 del 18.7.2008, pag. 37.

[4] Si veda anche il considerando 34 della direttiva 95/46. Su questo punto si veda inoltre il parere del Gruppo dell'articolo 29 sulle cartelle sanitarie elettroniche precedentemente citato (nota 8, punto 16).

pubblica e sulla salute e sicurezza sul luogo di lavoro ([1]), presenta un ulteriore rischio dovuto al diverso significato che i concetti di «segreto» e «protezione dei dati» possono assumere nell'ambito dell'applicazione, da un lato, della legislazione in materia di protezione dei dati e, dall'altro, della legislazione in materia di statistiche.

37. Il GEPD desidera sottolineare gli elementi suesposti nel contesto della proposta in esame. Dovrebbero essere inseriti riferimenti più espliciti ai requisiti in materia di protezione dei dati per quanto riguarda l'uso successivo dei dati sanitari (si veda la sezione III *infra*).

III. **ANALISI DETTAGLIATA DELLA PROPOSTA**

Le disposizioni in materia di protezione dei dati contenute nella proposta

38. La proposta fa riferimento alla protezione dei dati e alla tutela della vita privata in varie parti del documento; più precisamente:

— il considerando (3) afferma, tra l'altro, che la direttiva dev'essere attuata e applicata in conformità ai diritti al rispetto della vita privata e alla protezione dei dati di carattere personale;

— il considerando (11) fa riferimento al diritto fondamentale alla vita privata con riguardo al trattamento dei dati personali e alla riservatezza, due principi operativi condivisi dai sistemi sanitari di tutta la Comunità;

— il considerando (17) descrive il diritto alla protezione dei dati di carattere personale come diritto fondamentale della persona che andrebbe protetto, ponendo l'accento in particolare sul diritto di accesso del singolo ai propri dati personali relativi alla salute, anche nel contesto dell'assistenza sanitaria transfrontaliera, riconosciuto nella direttiva 95/46/CE;

— l'articolo 3, che stabilisce il rapporto della direttiva con altre disposizioni comunitarie, fa riferimento nel paragrafo 1, lettera a) alle direttive 95/46/CE e 2002/58/CE;

— l'articolo 5, relativo alle competenze dello Stato membro di cura, stabilisce nel paragrafo 1, lettera f) che rientra tra queste competenze la tutela del diritto alla vita privata, conformemente alle misure nazionali che attuano le direttive 95/46/CE e 2002/58/CE;

— l'articolo 6, relativo all'assistenza sanitaria prestata in un altro Stato membro, sottolinea nel paragrafo 5 il diritto dei pazienti che si recano in un altro Stato membro per avvalersi dell'assistenza sanitaria o che intendono avvalersi dell'assistenza sanitaria in un altro Stato membro ad accedere alla propria cartella clinica, anche in questo caso nel rispetto delle misure nazionali che attuano le direttive 95/46/CE e 2002/58/CE;

— l'articolo 12, relativo ai punti di contatto nazionali per l'assistenza sanitaria transfrontaliera, stabilisce nel paragrafo 2, lettera a) che questi punti di contatto hanno tra l'altro il compito di diffondere e fornire ai pazienti informazioni concernenti le garanzie in materia di protezione dei dati personali previste in un altro Stato membro;

— l'articolo 16, relativo alla sanità elettronica (*e-health*), afferma che le misure necessarie per realizzare l'interoperabilità dei sistemi basati sulle tecnologie dell'informazione e della comunicazione (TIC) devono rispettare il diritto fondamentale alla protezione dei dati personali conformemente alle norme applicabili;

— infine, nell'articolo 18, paragrafo 1, si stabilisce tra l'altro che la raccolta dei dati a fini statistici e di monitoraggio dev'essere effettuata nel rispetto delle norme nazionali e comunitarie sulla protezione dei dati personali.

39. Il GEPD constata con soddisfazione che nel redigere la proposta si è tenuto conto della protezione dei dati e si è tentato di evidenziare la necessità, in generale, di tutelare la vita privata nel contesto dell'assistenza sanitaria transfrontaliera. Tuttavia, le attuali disposizioni della proposta in materia di protezione dei dati o sono troppo generali o fanno riferimento alle competenze degli Stati membri in modo piuttosto selettivo e disorganico:

— in particolare, i considerando (3) e (11), come pure l'articolo 3, paragrafo 1, lettera a), l'articolo 16 e l'articolo 18, paragrafo 1 si riferiscono in realtà al quadro giuridico generale relativo alla protezione dei dati, gli ultimi due nel contesto della sanità elettronica (*e-health*) e della raccolta dei dati a fini statistici, senza tuttavia stabilire requisiti specifici in materia di tutela della vita privata;

— riguardo alle competenze degli Stati membri un riferimento generale è contenuto nell'articolo 5, paragrafo 1, lettera f);

— il considerando (17) e l'articolo 6, paragrafo 5 contengono un riferimento più specifico al diritto dei pazienti di accedere ai propri dati nello Stato membro di cura;

— infine, l'articolo 12, paragrafo 2, lettera a) contiene una disposizione relativa al diritto di informazione dei pazienti nello Stato membro di affiliazione (per il tramite dei punti di contatto nazionali).

Inoltre, come già affermato nell'introduzione del presente parere, non vi sono legami con gli aspetti relativi alla tutela della vita privata affrontati in altri strumenti giuridici comunitari (vincolanti o no) nel settore dell'assistenza sanitaria, specialmente con riguardo all'uso delle nuove applicazioni TIC (quali la telemedicina o le cartelle cliniche elettroniche), né è fatto riferimento a tali aspetti.

([1]) GU C 295 del 7.12.2007, pag. 1.

40. Pertanto, sebbene si faccia in generale riferimento alla tutela della vita privata come requisito dell'assistenza sanitaria transfrontaliera, continua a mancare un quadro d'insieme, sia in termini di obblighi degli Stati membri, sia in termini di specificità introdotte a motivo del carattere transfrontaliero della prestazione di servizi di assistenza sanitaria (rispetto alla prestazione di servizi di assistenza sanitaria in ambito nazionale). Più precisamente:

— le competenze degli Stati membri non sono presentate in modo integrato, dal momento che si fa riferimento ad alcuni obblighi (diritto di accesso e diritto di informazione), seppure in parti diverse della proposta, mentre non si fa il minimo accenno ad altri, quali la sicurezza del trattamento dei dati;

— non vi è alcun riferimento alle preoccupazioni che solleva l'incoerenza delle misure di sicurezza adottate dagli Stati membri e alla necessità di armonizzare i requisiti in materia di sicurezza dei dati sanitari a livello europeo, nel contesto dell'assistenza sanitaria transfrontaliera;

— non si fa alcun accenno all'integrazione della tutela della vita privata nelle applicazioni di sanità elettronica. Anche le disposizioni relative alle prescrizioni elettroniche non tengono conto in misura adeguata di questo aspetto.

41. Inoltre, l'articolo 18, relativo alla raccolta dei dati a fini statistici e di monitoraggio, suscita preoccupazioni specifiche. Il paragrafo 1 fa riferimento a «dati statistici e *altri dati complementari*»; dopo aver fatto inoltre riferimento a «fini di monitoraggio», al plurale, elenca i settori interessati da questi fini di monitoraggio, vale a dire la prestazione dell'assistenza sanitaria transfrontaliera, le cure erogate, i fornitori di questa assistenza e i pazienti, i costi e i risultati. In questo contesto, già poco chiaro, la disposizione contiene un riferimento generale alle norme in materia di protezione dei dati, senza tuttavia stabilire requisiti specifici in materia di uso successivo dei dati di carattere sanitario come disposto all'articolo 8, paragrafo 4 della direttiva 95/46/CE. Inoltre, il paragrafo 2 contiene l'obbligo incondizionato di trasferire alla Commissione almeno con cadenza annuale questa ingente mole di dati. Non essendovi riferimento esplicito a una valutazione della necessità di questo trasferimento, a quanto pare è il legislatore comunitario stesso ad aver già stabilito la necessità di questi trasferimenti alla Commissione.

Le raccomandazioni del GEPD

42. Per affrontare in maniera adeguata gli elementi sopra menzionati, il GEPD formula di seguito una serie di raccomandazioni consistenti in cinque fasi basilari di modifiche da apportare.

Fase 1 — Definizione di dati sanitari

43. L'articolo 4 definisce i termini di base utilizzati nella proposta. Il GEPD raccomanda vivamente di inserire in questo articolo una definizione di dati sanitari. Dovrebbe essere adottata un'interpretazione ampia di dati sanitari, sulla falsariga di quella descritta nella sezione II del presente parere (punti 14 e 15).

Fase 2 — Introduzione di un articolo specifico sulla protezione dei dati

44. Inoltre il GEPD raccomanda vivamente l'introduzione nella proposta di un articolo specifico sulla protezione dei dati, che potrebbe definire in modo chiaro e comprensibile la dimensione globale della tutela della vita privata. Detto articolo dovrebbe a) descrivere le competenze degli Stati membri di affiliazione e di cura, compresa — tra l'altro — la necessità della sicurezza del trattamento dei dati e b) individuare i principali settori di ulteriore sviluppo, per esempio l'armonizzazione in materia di sicurezza dei dati e l'integrazione della tutela della vita privata nella sanità elettronica. Per tali questioni possono essere previste disposizioni specifiche (nell'ambito dell'articolo proposto), quali presentate nelle fasi 3 e 4 infra.

Fase 3 — Disposizione specifica per l'armonizzazione in materia di sicurezza

45. A seguito della modifica di cui alla fase 2, il GEPD raccomanda che la Commissione adotti un meccanismo per la definizione di un livello di sicurezza comunemente accettabile per i dati sanitari a livello nazionale, tenuto conto delle norme tecniche esistenti in questo settore. Di questo si dovrebbe tener conto nella proposta. Ai fini dell'attuazione si potrebbe fare ricorso alla procedura di comitato, già descritta all'articolo 19 che si applica ad altre parti della proposta. Inoltre, ulteriori strumenti potrebbero essere utilizzati per la definizione delle pertinenti linee guida, coinvolgendo tutti i soggetti interessati, come il Gruppo dell'articolo 29 e il GEPD.

Fase 4 — Integrazione della tutela della vita privata nel modello di prescrizione elettronica

46. L'articolo 14 sul riconoscimento delle prescrizioni rilasciate in un altro Stato membro prevede l'elaborazione di un modello comunitario di prescrizione, in grado di supportare l'interoperabilità delle prescrizioni elettroniche. Questa misura è adottata tramite la procedura di comitato, quale definita all'articolo 19, paragrafo 2 della proposta.

47. Il GEPD raccomanda che il modello proposto di prescrizione elettronica integri i concetti di tutela della vita privata e di sicurezza dei dati, fin dalla definizione semantica di base di tale modello. Questo dovrebbe essere esplicitamente menzionato all'articolo 14, paragrafo 2, lettera a). Anche in questo caso il coinvolgimento di tutti i soggetti interessati riveste la massima importanza. A questo riguardo il GEPD desidera essere informato delle ulteriori azioni che saranno intraprese su tale argomento tramite la proposta procedura di comitato ed esservi coinvolto.

Fase 5 — Uso successivo dei dati sanitari a fini statistici e di monitoraggio

48. Per evitare malintesi, il GEPD incoraggia a precisare la nozione di «altri dati complementari» di cui all'articolo 18, paragrafo 1. L'articolo dovrebbe inoltre essere modificato in modo da riferirsi più esplicitamente ai requisiti per l'uso successivo dei dati sanitari quali stabiliti all'articolo 8, paragrafo 4 della direttiva 95/46/CE. L'obbligo di trasmettere tutti i dati alla Commissione, previsto nel paragrafo 2, dovrebbe altresì essere oggetto di una valutazione della necessità di tali trasferimenti per fini legittimi debitamente specificati in anticipo.

IV. **CONCLUSIONI**

49. Il GEPD desidera esprimere sostegno alle iniziative volte a migliorare le condizioni dell'assistenza sanitaria transfrontaliera. Esprime tuttavia perplessità sul fatto che le iniziative comunitarie in materia di assistenza sanitaria non siano sempre ben coordinate in relazione all'utilizzo delle TIC, alla tutela della vita privata e alla sicurezza dei dati, ostacolando in tal modo l'adozione di un approccio universale in materia di protezione dei dati nell'ambito dell'assistenza sanitaria.

50. Il GEPD si rallegra che nell'attuale proposta sia fatto riferimento alla tutela della vita privata. Tuttavia, sono necessarie varie modifiche, come spiegato nella sezione III del presente parere, per stabilire requisiti chiari, per gli Stati membri di cura e di affiliazione, e per affrontare correttamente la dimensione «protezione dei dati» dell'assistenza sanitaria transfrontaliera.

— Una definizione di dati sanitari dovrebbe essere inserita all'articolo 4, contemplando tutti i dati personali che possono avere un legame esplicito e stretto con la descrizione dello stato di salute di una persona. Questo dovrebbe includere in linea di massima dati medici, nonché dati amministrativi e finanziari in relazione alla salute.

— L'introduzione di un articolo specifico sulla protezione dei dati è vivamente raccomandata. Questo articolo dovrebbe stabilire chiaramente il quadro globale, descrivendo le competenze degli Stati membri di affiliazione e di cura e individuando i principali settori di ulteriore sviluppo, per esempio l'armonizzazione in materia di sicurezza dei dati e l'integrazione della tutela della vita privata, specialmente nelle applicazioni di sanità elettronica.

— Si raccomanda che la Commissione adotti, nell'ambito di tale proposta, un meccanismo per la definizione di un livello di sicurezza comunemente accettabile dei dati sanitari a livello nazionale, tenuto conto delle norme tecniche esistenti in questo settore. Dovrebbero inoltre essere incoraggiate iniziative supplementari e/o complementari, che coinvolgano tutti i soggetti interessati, il Gruppo dell'articolo 29 e il GEPD.

— Si raccomanda che la nozione di «tutela della vita privata fin dalla progettazione» sia inserita nel modello comunitario proposto di prescrizione elettronica (anche a livello semantico). Questo dovrebbe essere esplicitamente menzionato all'articolo 14, paragrafo 2, lettera a). Il GEPD desidera essere informato delle ulteriori azioni che saranno intraprese su tale argomento tramite la proposta procedura di comitato ed esservi coinvolto.

— Si raccomanda di rendere più precisa la formulazione dell'articolo 18 e di includere un riferimento più esplicito ai requisiti specifici in materia di uso successivo dei dati di carattere sanitario come disposto all'articolo 8, paragrafo 4 della direttiva 95/46/CE.

Fatto a Bruxelles, il 2 dicembre 2008.

Peter HUSTINX

Garante europeo della protezione dei dati

Secondo parere del Garante europeo della protezione dei dati sulla revisione della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

(2009/C 128/04)

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,

vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche,

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

1. Il 13 novembre 2007, la Commissione europea ha adottato una proposta che modifica, tra l'altro, la direttiva relativa alla vita privata e alle comunicazioni elettroniche, nota anche come direttiva e-privacy [1] (in prosieguo «proposta» o «proposta della Commissione»). Il 10 aprile 2008, il GEPD ha adottato un parere sulla proposta della Commissione in cui forniva raccomandazioni volte a migliorare la proposta nell'intento di contribuire ad assicurare che le modifiche proposte si traducessero nella migliore possibile protezione della vita privata e dei dati delle persone («primo parere del GEPD») [2].

2. Il GEPD ha accolto favorevolmente la proposta della Commissione di istituire un sistema obbligatorio di notificazione delle violazioni di sicurezza che obbliga le società a informare le persone qualora i loro dati personali siano stati compromessi. Ha inoltre elogiato la nuova disposizione che permette alle persone giuridiche (per es. associazioni di consumatori e fornitori di servizi Internet) di promuovere azioni giudiziarie contro i mittenti di comunicazioni commerciali indesiderate (spammer) in modo da integrare ulteriormente gli strumenti esistenti di lotta alle comunicazioni indesiderati.

3. Durante il dibattito parlamentare che ha preceduto la prima lettura del Parlamento europeo, il GEPD ha formulato un ulteriore parere formulando osservazioni su quesiti specifici emersi nelle relazioni redatte dalle commissioni del Parlamento europeo competenti per la revisione delle direttive servizio universale [3] e e-privacy («Osservazioni») [4]. Le osservazioni riguardavano in primo luogo problemi connessi al trattamento di dati relativi al traffico e la protezione dei diritti di proprietà intellettuale.

4. Il 24 settembre 2008, il Parlamento europeo («PE») ha adottato una risoluzione legislativa sulla direttiva e-privacy («prima lettura») [5]. Il GEPD ha valutato positivamente vari emendamenti del PE che sono stati adottati in seguito al parere del GEPD e alle osservazioni succitate. Tra le importanti modifiche figura l'inclusione dei fornitori di servizi della società dell'informazione (ossia le imprese operanti in Internet) nell'ambito di applicazione dell'obbligo di notificare le violazioni di sicurezza. Il GEPD ha anche accolto favorevolmente l'emendamento che

[1] La revisione della direttiva e-privacy è parte di un più ampio processo di riesame inteso alla creazione di un'autorità per le telecomunicazioni a livello di UE, al riesame delle direttive 2002/21/EC, 2002/19/EC, 2002/20/EC, 2002/22/EC e 2002/58/EC, nonché al riesame del regolamento (CE) n. 2006/2004 (in appresso «riesame del pacchetto telecomunicazioni» per l'insieme degli strumenti giuridici).

[2] Parere del 10 aprile 2008 sulla proposta di direttiva recante modifica, tra l'altro, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) GU C 181 del 18.7.2008, pag. 1.

[3] Direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva servizio universale), GU L 108, del 24.4.2002, pag. 51.

[4] Osservazioni del GEPD su quesiti specifici emersi dalla relazione IMCO sulla revisione della direttiva 2002/22/EC (servizio universale) e direttiva 2002/58/CE (e-privacy), 2 settembre 2008. Disponibile all'indirizzo: www.edps.europa.eu

[5] Risoluzione legislativa del Parlamento europeo del 24 settembre 2008 sulla proposta di direttiva del Parlamento europeo e del Consiglio recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione per la tutela dei consumatori [COM(2007) 698 – C6-0420/2007 2007/0248(COD)].

consente alle persone giuridiche e fisiche di promuovere azioni giudiziarie in caso di violazione di qualsiasi disposizione della direttiva e-privacy (non solo in caso di violazione delle disposizioni in materia di spam come proposto inizialmente nella proposta della Commissione). La prima lettura del Parlamento è stata seguita dall'adozione da parte della Commissione di una proposta che modifica la direttiva e-privacy (in prosieguo «proposta modificata») ([6]).

5. Il 27 novembre 2008 il Consiglio ha raggiunto un accordo politico su un riesame delle norme sul pacchetto telecomunicazioni, compresa la direttiva e-privacy, destinato a diventare la posizione comune del Consiglio («posizione comune») ([7]). La posizione comune sarà notificata al PE ai sensi dell'articolo 251, paragrafo 2 del trattato che istituisce la Comunità europea, il che può comportare la proposta di emendamenti da parte del PE.

Parere generale sulla posizione del Consiglio

6. Il Consiglio ha modificato elementi essenziali del testo della proposta e non ha accettato molti degli emendamenti adottati dal PE. È vero che la posizione comune contiene certamente elementi positivi, ma nell'insieme il GEPD è preoccupato per il suo contenuto, in particolare poiché la posizione comune non tiene conto di alcuni degli emendamenti positivi proposti dal PE, della proposta modificata o dei pareri del GEPD e delle autorità europee preposte alla protezione dei dati emessi tramite il gruppo dell'articolo 29 ([8]).

7. Al contrario, in alcuni casi le disposizioni della proposta modificata e degli emendamenti del PE che prevedono garanzie per i cittadini sono state soppresse o indebolite in modo sostanziale. Ne risulta una sostanziale riduzione del livello di protezione offerto alle persone nella posizione comune. Ciò ha indotto il GEPD a emettere un secondo parere, nella speranza che nel corso del processo legislativo sulla direttiva e-privacy siano adottati nuovi emendamenti che ripristinino le garanzie in materia di protezione dei dati.

8. Questo secondo parere è incentrato su alcune preoccupazioni essenziali e non riprende tutti i punti sollevati nel primo parere del GEPD o nelle osservazioni, che rimangono tutti validi. Il presente parere riguarda in particolare i punti seguenti:

— le disposizioni relative alla notifica delle violazioni di sicurezza;

— la portata dell'applicazione della direttiva e-privacy alle reti private e alle reti private accessibili al pubblico;

— il trattamento dei dati relativi al traffico a fini di sicurezza;

— la possibilità offerta alle persone giuridiche di promuovere azioni giudiziarie in caso di violazione della direttiva e-privacy.

9. Nell'affrontare le tematiche succitate, il presente parere analizza la posizione comune del Consiglio e la confronta con la prima lettura del PE e la proposta modificata della Commissione. Il parere contiene raccomandazioni intese a semplificare le disposizioni della direttiva e-privacy e ad assicurare che la direttiva continui a protegge adeguatamente la vita privata e i dati personali.

II. LE DISPOSIZIONI RELATIVE ALLA NOTIFICAZIONE DI VIOLAZIONI DI SICUREZZA

10. Il GEPD sostiene l'adozione di un sistema di notificazione delle violazioni di sicurezza in base al quale alle autorità e alle persone viene data comunicazione qualora i loro dati personali siano stati compromessi ([9]). Le comunicazioni relative a violazioni di sicurezza possono aiutare le persone ad adottare le necessarie misure per attenuare qualsiasi danno potenziale risultante dalla compromissione dei dati. L'obbligo di inviare comunicazioni su violazioni di sicurezza incoraggerà inoltre le società a migliorare la sicurezza dei dati e ad aumentare la loro responsabilità riguardo ai dati personali di cui sono responsabili.

11. La proposta modificata della Commissione, la prima lettura del Parlamento e la posizione comune del Consiglio presentano tre approcci diversi alla notifica di violazioni di sicurezza attualmente all'esame. Ciascuno dei tre approcci ha aspetti positivi. Il GEPD ritiene tuttavia che vi siano possibilità di miglioramento in ciascuno di essi e consiglia di prendere in considerazione le raccomandazioni descritte in appresso nell'esame delle fasi finali in vista dell'adozione di un sistema riguardante le violazioni di sicurezza.

([6]) Proposta modificata di direttiva del Parlamento europeo e del Consiglio recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione per la tutela dei consumatori, Bruxelles 6.11.2008, COM(2008) 723 def.

([7]) Disponibile sul sito web pubblico del Consiglio.

([8]) Parere 2/2008 sul riesame della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche (direttiva e-privacy), disponibile sul sito web del gruppo dell'articolo 29.

([9]) Nel presente parere è usata la parola «compromessi» in riferimento alle violazioni di dati personali verificatesi in seguito a distruzione, perdita, modifica, rivelazione non autorizzata o accesso, accidentalmente o in modo illecito, in riferimento a dati personali trasmessi, memorizzati o comunque elaborati.

12. Nell'analisi dei tre sistemi di notificazione di violazioni di sicurezza, vanno presi in considerazione cinque punti fondamentali: *i)* la definizione di violazione di sicurezza; *ii)* i soggetti contemplati dall'obbligo di notifica («soggetti contemplati»); *iii)* il criterio che dà luogo all'obbligo di notificazione; *iv)* l'individuazione del soggetto competente per determinare se una violazione di sicurezza soddisfa o non soddisfa il criterio e v) i destinatari dell'informazione.

Panoramica degli approcci della Commissione, del Consiglio e del Parlamento

13. Il Parlamento europeo, la Commissione e il Consiglio hanno adottato differenti approcci per la notificazione di violazioni di sicurezza La prima lettura del PE ha modificato il sistema originario di notificazione di violazioni di sicurezza previsto dalla proposta della Commissione ([10]). In base all'approccio del PE l'obbligo di notificazione non si applica solo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico ma anche ai fornitori di servizi della società dell'informazione («PPECS» e «ISSP»). Inoltre, in base a questo approccio tutte le violazioni di dati personali dovrebbero essere notificate all'autorità nazionale di regolamentazione o alle autorità competenti (insieme «autorità»). Se dovessero determinare che la violazione è *grave*, le autorità competenti richiederebbero ai PPECS e agli ISSP di notificare senza indugio la violazione alle persone che ne sono interessate. In caso di violazioni che rappresentano un pericolo imminente e diretto, i PPECS e gli ISSP informerebbero le persone prima di informare le autorità e non attenderebbero una determinazione normativa. Un'eccezione all'obbligo di informare i consumatori si applica ai soggetti che possono dimostrare alle autorità che sono state applicate appropriate misure di protezione tecnica atte a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

14. Anche in base all'approccio del Consiglio, la notificazione deve essere fornita sia agli abbonati che alle autorità, ma solo qualora il soggetto contemplato ritenga che la violazione costituisca un rischio grave per la vita privata dell'abbonato (ossia furto o usurpazione d'identità, danno fisico, umiliazione grave o danno alla reputazione).

15. La proposta modificata della Commissione mantiene l'obbligo proposto dal PE di notificare alle autorità tutte le violazioni. Tuttavia, a differenza dell'approccio del Parlamento, la proposta modificata contiene una deroga all'obbligo della notificazione per quanto riguarda le persone interessate qualora il PPECS dimostri all'autorità competente che *i)* «*è ragionevolmente improbabile*» che la violazione comporti una lesione (ad esempio danni economici e sociali o furti di identità) o *ii)* ai dati interessati dalla violazione sono state applicate «*opportune misure di protezione tecnologica*». L'approccio della Commissione include pertanto un'analisi basata sui danni in collegamento con le singole notifiche.

([10]) In particolare, gli emendamenti 187, 124-127 nonché 27, 21 e 32 del PE affrontano tale questione.

16. È importante notare che in base agli approcci del Parlamento ([11]) e della Commissione sono le autorità ad essere in definitiva incaricate di determinare se la violazione sia grave o vi sia una probabilità ragionevole che causi danni. Secondo l'approccio del Consiglio la decisione è invece rimessa ai soggetti interessati.

17. Sia l'approccio del Consiglio che quello della Commissione si applicano soltanto ai PPECS e non, come l'approccio del Parlamento, agli ISSP.

La definizione di violazione di sicurezza

18. Il GEPD è lieto di constatare che le tre proposte legislative contengono la stessa definizione di notifica della violazione di sicurezza descritta come «*violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati […]*» ([12]).

19. Come descritto meglio in appresso, questa definizione è accolta favorevolmente in quanto abbastanza generale per abbracciare la maggior parte delle situazioni pertinenti in cui la notificazione di violazioni di sicurezza può essere giustificata.

20. In primo luogo, nella definizione rientrano casi in cui si sia verificato un accesso non autorizzato ai dati personali da parte di terzi, quali la penetrazione in un server contenente dati personali e l'estrazione di tali informazioni.

21. In secondo luogo, la definizione includerebbe anche situazioni in cui si sia verificata la perdita, o la rivelazione di dati personali, anche se l'accesso non autorizzato non è ancora stato dimostrato. Vi rientrerebbero situazioni in cui i dati personali possono essere stati smarriti (per es. CD ROM, chiavi USB o altri dispositivi portatili), o resi disponibili al pubblico da utenti regolari (file di dati sui dipendenti resi inavvertitamente e temporaneamente disponibili in uno spazio accessibile al pubblico via Internet). Poiché spesso non sarà possibile provare che in un determinato momento è o non è possibile che terzi non autorizzati accedano a tali dati o li utilizzino, sembra appropriato includere queste fattispecie nell'ambito della definizione. Il GEPD raccomanda pertanto di mantenere questa definizione. Raccomanda anche di includere la definizione di violazione di sicurezza all'articolo 2 della direttiva e-privacy in quanto ciò sarebbe più coerente con la struttura generale della direttiva e fornirebbe maggiore chiarezza.

([11]) Eccetto qualora esista un pericolo imminente e diretto, nel qual caso i soggetti contemplati devono informare prima i consumatori.

([12]) Articolo 2, lettera i) della posizione comune e della proposta modificate e articolo 3, paragrafo 3 della prima lettura del Parlamento.

Soggetti ai quali dovrebbe essere imposto l'obbligo della notificazione

22. In base all'approccio del PE, l'obbligo di notificazione si applica sia ai PPECS che agli ISSP. Tuttavia, secondo i regimi previsti dal Consiglio e dalla Commissione, solo PPECS quali le società di telecomunicazione e i fornitori di accesso a Internet saranno obbligati a informare le persone qualora subiscano violazioni di sicurezza che comportano la compromissione di dati personali. Altri settori di attività, per esempio le banche in linea, i rivenditori in linea, i fornitori di servizi sanitari in linea e altri non sono vincolati da questo obbligo. Per i motivi succitati, il GEPD ritiene che dal punto di vista dell'interesse pubblico sia fondamentale assicurare che anche i servizi della società dell'informazione che includono il commercio in linea, le banche in linea, i fornitori di servizi sanitari in linea ecc. siano soggetti all'obbligo di notificazione.

23. In primo luogo, il GEPD rileva che benché le società di telecomunicazione siano certamente oggetto di violazioni di sicurezza che giustificano un obbligo di notificazione, lo stesso vale per altri tipi di società/fornitori. Anche i rivenditori in linea, le banche in linea, le farmacie in linea possono subire violazioni di sicurezza alla stessa stregua delle società di telecomunicazione, se non in misura maggiore. Pertanto, considerato il rischio, non è opportuno limitare ai PPECS l'obbligo di notificazione di una violazione. L'esigenza di un approccio più ampio è corroborato dalle esperienze acquisite in altri paesi. Per esempio, negli Stati Uniti quasi tutti gli Stati (attualmente oltre 40) hanno varato leggi sulla notificazione di violazioni di sicurezza che hanno un campo d'applicazione più ampio, che comprende non solo i PPECS ma qualsiasi soggetto che detiene i dati personali richiesti.

24. In secondo luogo, se una violazione dei tipi di dati personali regolarmente trattati dai PPECS può chiaramente incidere sulla vita privata di una persona, lo stesso vale, forse a maggior ragione, per i tipi di informazioni trattate dagli ISSP. Certamente le banche e altri istituti finanziari possono essere in possesso di informazioni altamente riservate (per es. dettagli di conti bancari), la cui divulgazione può dar luogo a un uso a fini di usurpazione dell'identità. Anche la divulgazione di informazioni assai sensibili attinenti alla salute da parte di servizi sanitari in linea può essere particolarmente dannosa per le persone. Pertanto, anche i tipi di dati personali che possono essere compromessi richiedono una più ampia applicazione della notificazione di violazione di sicurezza che includerebbe, come minimo, gli ISSP.

25. Sono stati sollevati alcuni problemi di natura giuridica riguardo all'ampliamento del campo d'applicazione di questo articolo, ossia i soggetti contemplati dall'obbligo in questione. In particolare il fatto che il campo d'applicazione generale della direttiva e-privacy riguardi solo i PPECS è stato addotto come ostacolo all'applicazione dell'obbligo di notificare anche agli ISSP.

26. In questo contesto il GEPD tiene a ricordare quanto segue: *i)* non esiste nessun tipo di ostacolo all'inclusione di attori diversi dai PPECS nel campo di applicazione di determinate disposizioni della direttiva. Il legislatore comunitario dispone di un potere discrezionale illimitato a tale riguardo; *ii)* nella vigente direttiva e-privacy esistono altri precedenti di applicazione a soggetti diversi dai PPECS.

27. Per esempio, l'articolo 13 si applica non solo ai PPECS ma a qualsiasi società che invia comunicazioni non richieste, prescrivendo un consenso «opt-in» preliminare a tal fine. Inoltre, l'articolo 5, paragrafo 3 della direttiva e-privacy che vieta, tra l'altro, la memorizzazione di informazioni quali cookie nei terminali degli utenti è vincolante non solo per i PPECS ma anche per chiunque tenti di memorizzare informazioni o ottenere l'accesso alle informazioni memorizzate nell'apparecchiatura terminale delle persone. Per giunta, nel processo legislativo in corso, la Commissione ha addirittura proposto di estendere l'applicazione dell'articolo 5, paragrafo 3 ai casi in cui tecnologie analoghe (cookie/software spia) siano forniti non solo tramite sistemi di comunicazione elettronica ma anche tramite qualsiasi altro metodo possibile (distribuzione attraverso software provenienti da Internet oppure attraverso supporti esterni per la memorizzazione dei dati, quali CD-ROM, chiavi USB, unità flash ecc.). Tutti questi elementi sono positivi e dovrebbero essere mantenuti, ma anche costituire precedenti per l'attuale discussione sul campo d'applicazione.

28. Inoltre, nell'attuale processo legislativo, la Commissione e il PE e presumibilmente il Consiglio hanno proposto un nuovo articolo 6, paragrafo 6, lettera a) discusso in appresso, che si applica a soggetti diversi dai PPECS.

29. Infine, tenuto conto degli elementi generalmente positivi derivanti dall'obbligo di notificare violazioni di sicurezza, è molto probabile che i cittadini si aspettino questi vantaggi non solo qualora i loro dati personali siano stati compromessi da PPECS ma anche qualora ciò sia avvenuto ad opera di ISSP. Le attese dei cittadini potrebbero essere deluse se, ad esempio, non venissero informati qualora una banca in linea abbia smarrito le informazioni sul loro conto bancario.

30. In definitiva, il GEPD è convinto che la notificazione di violazioni di sicurezza potrà produrre tutti i suoi effetti positivi solo se i soggetti contemplati comprenderanno sia i PPECS che gli ISSP.

Il criterio che dà luogo alla notificazione

31. Per quanto riguarda l'attivazione della notificazione, come spiegato dettagliatamente in appresso, il GEPD ritiene che il criterio della proposta modificata «*ragionevolmente probabile che possa ledere*» sia il più appropriato dei tre criteri proposti. Tuttavia, è importante far sì che il concetto di «ledere» sia sufficientemente ampio da contemplare tutte le pertinenti fattispecie di effetti negativi sulla vita privata o su altri interessi legittimi delle persone. Altrimenti sarebbe preferibile introdurre un nuovo criterio in base al quale la notificazione sarebbe obbligatoria «*se vi è una probabilità ragionevole che la violazione produca effetti negativi per le persone*».

32. Come accennato nella sezione precedente, le condizioni alle quali deve essere data comunicazione alle persone (denominati «attivazione» e «criterio») sono diversi nell'ambito degli approcci del PE, della Commissione e del Consiglio. È ovvio che la quantità delle comunicazioni che le persone riceveranno dipenderà, in larga misura, dall'attivazione o dal criterio fissati per la notificazione.

33. In base all'approccio del Consiglio e della Commissione, la notificazione deve essere effettuata se la violazione costituisce una «grave violazione della vita privata dell'abbonato» (Consiglio) e se «*è ragionevolmente probabile che la violazione possa ledere gli interessi del consumatore*» In base all'approccio del PE, l'attivazione per la notificazione alle persone è data dalla «gravità della violazione» (ossia la notifica alle persone è richiesta se la violazione è considerata «grave»). Al di sotto di tale soglia non è necessaria la notificazione ([13])

34. Il GEPD comprende che si può sostenere che, se sono stati compromessi dati personali, le persone ai quali appartengono i dati hanno il diritto di venirne a conoscenza in qualsiasi circostanza. Ma è corretto ponderare se ciò sia una soluzione appropriata alla luce di altri interessi e considerazioni.

35. È stato affermato che l'obbligo di inviare comunicazioni ogniqualvolta siano stati compromessi dati personali, in altre parole senza limitazioni, può comportare un eccesso di notificazioni e «stanchezza da comunicazioni» il che potrebbe tradursi in desensibilizzazione. Come precisato in appresso, il GEPD è sensibile a questo argomento; tuttavia tiene a sottolineare la sua preoccupazione per il fatto che l'eccesso di notificazioni è un possibile indicatore di diffuse carenze nelle prassi in materia di sicurezza dell'informazione.

([13]) Cfr. nota 11 relativa alla deroga a tale norma.

36. Come indicato in precedenza, il GEPD ravvisa potenziali conseguenze negative nell'eccesso di notificazioni e desidera contribuire ad assicurare che il quadro giuridico adottato per la notificazione di violazioni di sicurezza non produca questo risultato. Se le persone dovessero ricevere frequenti comunicazioni di violazione anche in situazioni in cui non vi sono effetti negativi, danni o pericoli, può andare a finire che venga messo a repentaglio uno degli obiettivi fondamentali della comunicazione in quanto, paradossalmente, le persone potrebbero ignorare comunicazioni in casi in cui potrebbero effettivamente dover intervenire per proteggersi. È quindi importante trovare un giusto equilibrio nel fornire comunicazioni sensate poiché, se le persone non reagiscono alle comunicazioni ricevute, l'efficacia dei sistemi di notificazione è fortemente ridotta.

37. Al fine di adottare un criterio appropriato che non porti a un eccesso di notificazioni, vanno esaminati, oltre all'attivazione della comunicazione, altri fattori, in particolare la definizione di violazione di sicurezza e l'informazione oggetto dell'obbligo di notificazione. A tale riguardo il GEPD rileva che in base ai tre approcci proposti, è possibile avere una gran quantità di notificazioni tenuto conto dell'ampia definizione di violazione di sicurezza succitata. Questa preoccupazione per un eccesso di notificazioni è ulteriormente sottolineata dal fatto che la definizione di violazione di sicurezza si applica a tutti i tipi di dati personali. Benché il GEPD ritenga che questo sia l'approccio corretto (che non limita i tipi di dati personali soggetti a notificazione), contrariamente ad altri approcci quali le leggi USA in cui i requisiti sono incentrai sulla sensibilità dell'informazione, si tratta comunque di un fattore di cui tener conto.

38. Alla luce di quanto indicato sopra e tenendo conto delle diverse variabili esaminate nel loro insieme, il GEPD ritiene appropriato includere una soglia o criterio al di sotto del quale la notificazione non è obbligatoria.

39. I criteri proposti secondo cui la violazione deve rappresentare un «*rischio grave per la vita privata*» o è «*ragionevolmente probabile che possa ledere*» sembrano entrambi includere, per esempio, danni sociali, alla reputazione o economici. Per esempio questi criteri riguarderebbero casi di esposizione a usurpazione dell'identità mediante la divulgazione di identificatori non pubblici quali i numeri di passaporto, nonché la rivelazione di informazioni sulla vita privata di una persona. Il GEPD è favorevole a questa impostazione. È convinto che non sarebbero realizzati tutti i possibili effetti positivi della notificazione di violazioni di sicurezza se il sistema di notificazione contemplasse solo le violazioni che comportano danni economici.

40. Tra i due criteri proposti, il GEPD preferisce il criterio proposto dalla Commissione «*ragionevolmente probabile che possa ledere*» in quanto offrirebbe un livello più appropriato di protezione delle persone. È molto più probabile che le violazioni giustifichino una notificazione qualora sia «*ragionevolmente probabile che possano ledere*» la vita privata delle persone che qualora presentino «*un grave rischio*» di lesione. Pertanto, contemplando solo le violazioni che presentano un grave rischio per la vita privata delle persone si limiterebbe considerevolmente il numero delle violazioni che devono essere notificate. Contemplando solo questo genere di violazioni si conferirebbe ai PPECS e agli ISSP un potere discrezionale smodato per quanto riguarda la necessità di emettere una notificazione, in quanto sarebbe molto più facile per loro giustificare la conclusione secondo cui non esiste «nessun *rischio grave*» che la conclusione secondo cui è «*ragionevolmente improbabile che si verifichi*» una lesione. È vero che occorre comunque evitare un eccesso di notifiche, ma in compenso deve essere concesso il beneficio del dubbio al fine di proteggere l'interesse delle persone alla loro vita privata e il limite minimo per la protezione delle persone è dato dal momento in cui è ragionevolmente probabile che una violazione causi loro dei danni. Inoltre i termini «*ragionevolmente probabile*» saranno più efficaci nell'applicazione pratica, sia per i soggetti contemplati che per le autorità competenti, in quanto richiedono una valutazione oggettiva del caso e del relativo contesto.

41. Le violazioni riguardanti dati personali possono inoltre creare danni che sono difficilmente quantificabili e possono essere di diversa natura. Infatti, la divulgazione dello stesso tipo di dati può, a seconda delle circostanze specifiche, provocare danni significativi a una persona e minori a un'altra. Non sarebbe appropriato un criterio secondo cui il danno deve essere materiale, significativo o grave. Per esempio, l'approccio del Consiglio secondo cui la violazione deve pregiudicare *gravemente* la vita privata di una persona, fornirebbe una protezione inadeguata ai singoli nella misura in cui tale criterio richiede che l'effetto sulla vita privata sia «grave». Ciò dà altresì adito a una valutazione soggettiva.

42. Mentre, come precedentemente descritto, il criterio: «*ragionevolmente probabile che possa ledere*» sembra essere appropriato per la notificazione di violazione di sicurezza, il GEPD continua a nutrire la preoccupazione che esso non possa includere tutte le situazioni in cui è giustificata una comunicazione alle persone, ossia tutte le situazioni in cui vi è una probabilità ragionevole di effetti negativi sulla vita privata o su altri interessi legittimi delle persone. Per tale motivo potrebbe essere preso in considerazione un criterio che darebbe luogo alla notificazione «*se vi è una probabilità ragionevole che la violazione produca effetti negativi per le persone*».

43. Questo criterio alternativo presenta l'ulteriore vantaggio della conformità alla normativa dell'UE in materia di protezione dei dati. In effetti, la direttiva sulla tutela dei dati fa spesso riferimento ad effetti negativi sui diritti e le libertà degli interessati. Per esempio, l'articolo 18 e il considerando 49, che riguardano l'obbligo di registrare le operazioni di trattamento dei dati presso le autorità preposte alla protezione dei dati, autorizzano gli Stati membri a derogare a tale obbligo qualora i trattamenti non siano «*tali da recare pregiudizio ai diritti e alle libertà delle persone interessate*» Termini analoghi figurano all'articolo 16, paragrafo 6 della posizione comune che autorizza le persone giuridiche a promuovere azioni giudiziarie contro coloro che inviano messaggi di posta elettronica indesiderata (spammer).

44. Inoltre, tenendo conto di quanto precede, ci si aspetterebbe anche che i soggetti contemplati e in particolare le autorità competenti a mettere in atto la normativa in materia di protezione dei dati avessero maggiore familiarità con il criterio suddetto, facilitando in tal modo la valutazione se una determinata violazione soddisfi il criterio previsto.

Soggetto competente per determinare se una violazione di sicurezza soddisfa o non soddisfa il criterio

45. In base all'approccio del PE (fatta eccezione per i casi di pericolo imminente) e alla proposta modificata della Commissione, spetta alle autorità degli Stati membri determinare se una violazione di sicurezza soddisfi il criterio di attivazione dell'obbligo di notificazione agli interessati.

46. Il GEPD ritiene che il coinvolgimento di un'autorità svolga un ruolo importante nel determinare se un criterio è soddisfatto in quanto ciò è, in una certa misura, una garanzia per la corretta applicazione della legge. Questo sistema può impedire che le società, in modo inappropriato, considerino la violazione non lesiva/grave evitando in tal modo la notificazione allorché, in effetti, tale notificazione è necessaria.

47. D'altro canto, il GEPD nutre preoccupazione per il fatto che un regime secondo il quale le autorità sono incaricate di effettuare la valutazione può essere poco pratico e di difficile applicazione, o può nella prassi rivelarsi controproducente. Può addirittura diminuire le garanzie in materia di protezione dei dati per le persone.

48. Infatti, in base a tale approccio le autorità preposte alla protezione dei dati verranno probabilmente inondate da notificazioni di violazioni di sicurezza e potranno incontrare gravi difficoltà nell'effettuare le necessarie valutazioni. È importante ricordare che per valutare se una violazione soddisfa il criterio previsto, le autorità dovranno disporre di sufficienti informazioni interne, spesso di natura tecnica complessa, che dovranno trattare molto rapidamente. Tenendo conto della difficoltà di valutazione e del fatto che alcune autorità dispongono di risorse limitate, il GEPD teme che sarà assai difficile per le autorità adempiere a questo obbligo e che saranno loro sottratte risorse necessarie per altre priorità importanti. Inoltre, tale sistema può esercitare un'indebita pressione sulle autorità; in effetti, se esse decidono che la violazione non è grave e ciò nonostante le persone subiscono dei danni, le autorità potrebbero essere ritenute responsabili.

49. Questa difficoltà è ulteriormente evidenziata se si tiene conto del fatto che il tempo è un fattore determinante nel ridurre al minimo i rischi derivanti da violazioni di sicurezza. A meno che le autorità siano in grado di effettuare la valutazione entro un lasso di tempo assai breve, l'ulteriore tempo richiesto affinché le autorità possano effettuare tali valutazioni può aumentare i danni subiti dagli interessati. Pertanto, questo intervento aggiuntivo che è inteso a fornire una maggiore protezione alle persone può, paradossalmente, tradursi in una minore protezione rispetto ai sistemi basati sulla notificazione diretta.

50. Per i motivi succitati, il GEPD ritiene che sia preferibile istituire un sistema secondo il quale spetterebbe ai soggetti interessati valutare se la violazione soddisfi o non soddisfi il pertinente criterio, come previsto nell'approccio del Consiglio.

51. Tuttavia, per evitare rischi di possibili abusi, per esempio da parte di soggetti che rifiutano la notificazione in circostanze in cui essa è chiaramente dovuta, è estremamente importante includere determinate garanzie in materia di protezione dei dati che sono descritte in appresso

52. In primo luogo, l'obbligo imposto ai soggetti contemplati di determinare se devono effettuare la notificazione deve evidentemente essere accompagnato da un altro obbligo relativo alla notificazione obbligatoria alle autorità di tutte le violazioni che soddisfano il criterio stabilito. I soggetti interessati dovrebbero in questi casi essere obbligati a informare le autorità della violazione e dei motivi della loro decisione riguardante la notificazione nonché del contenuto di tutte le notificazioni effettuate.

53. In secondo luogo, alle autorità deve essere conferito un effettivo ruolo di supervisione. Nell'esercitare questo ruolo, le autorità devono avere la facoltà, ma non l'obbligo, di indagare sulle circostanze della violazione e imporre qualsiasi misura necessaria per porvi rimedio ([14]). Ciò dovrebbe includere non solo la comunicazione alle persone (se non ha già avuto luogo) ma anche la facoltà di imporre l'obbligo di intervenire per impedire ulteriori violazioni. Alle autorità dovrebbero essere attribuiti effettivi poteri e risorse a tale riguardo nonché il necessario margine di discrezionalità per decidere quando reagire a una notificazione riguardante una violazione di sicurezza. In altre parole, ciò consentirebbe alle autorità di essere selettive ed effettuare indagini su, per esempio, violazioni di sicurezza di vasta portata e veramente dannose, verificando e imponendo l'ottemperanza a quanto prescrive la legge.

54. Per conseguire l'obiettivo succitato, in aggiunta ai poteri conferiti dalla direttiva e-privacy nonché dall'articolo 15 bis, paragrafo 3 e dalla direttiva sulla tutela dei dati, il GEPD raccomanda di inserire il testo seguente: «*Se l'abbonato o il singolo interessato non ha ancora ricevuto la notificazione, le autorità nazionali competenti, considerata la natura della violazione, possono chiedere ai PPECS o agli ISSP di provvedere alla notificazione*».

55. Il GEPD raccomanda inoltre al PE e al Consiglio di confermare l'obbligo proposto dal PE (emendamento 122, articolo 4, paragrafo 1, lettera a) che i soggetti effettuino una valutazione e identificazione dei rischi riguardo ai loro sistemi e ai dati personali che intendono trattare. In base a questo obbligo, i soggetti dovrebbero elaborare una definizione adeguata e accurata delle misure di sicurezza che saranno applicate nei casi che li riguardano, che dovrebbe essere a disposizione delle autorità. In caso di violazione di sicurezza, questo obbligo aiuterà i soggetti contemplati — e in definitiva anche le autorità nell'espletamento della loro funzione di supervisione — a determinare se la compromissione di tali informazioni può provocare effetti negativi o danni alle persone.

56. In terzo luogo, l'obbligo imposto ai soggetti contemplati di determinare se devono effettuare notificazioni alle persone deve essere accompagnato da un obbligo di mantenere piste di controllo interno dettagliate e globali con la descrizione di tutte le violazioni verificatesi e di tutte le relative notificazioni nonché di tutte le misure prese per evitare future violazioni. Queste piste di controllo interno devono essere a disposizione delle autorità per l'esame e le eventuali indagini. Ciò consentirà alle autorità di espletare le loro funzioni di supervisione. Ciò potrebbe essere conseguito con l'adozione di un testo del tenore seguente: «*I PPECS e gli ISSP effettuano e conservano una registrazione completa e dettagliata di tutte le violazioni di sicurezza occorse, delle pertinenti informazioni tecniche ad esse collegate e delle misure adottate per porvi rimedio. I registri contengono altresì un riferimento a tutte le notificazioni effettuate agli abbonati o ai singoli interessati nonché alle autorità nazionali competenti, inclusi le relative date e il relativo contenuto. I registri sono prodotti all'autorità nazionale competente a sua richiesta*».

57. Naturalmente, al fine di assicurare la coerenza nell'attuazione di questa norma nonché di altri aspetti pertinenti del quadro relativo alla violazione di sicurezza, come il formato e la procedura per la notificazione, è opportuno che la Commissione adotti misure tecniche di attuazione, previa consultazione del GEPD, del Gruppo dell'articolo 29 e di altri pertinenti soggetti interessati.

([14]) L'articolo 15 bis, paragrafo 3 riconosce questa facoltà di supervisione prevedendo che «*Gli Stati membri provvedono affinché le autorità nazionali competenti e, se del caso, altri organismi nazionali, dispongano di tutte le risorse e di tutte le competenze necessarie, compresa la possibilità di ottenere ogni informazione pertinente di cui possano avere bisogno per applicare e controllare le disposizioni nazionali adottate conformemente alla presente direttiva*».

Destinatari della notificazione

58. Per quanto riguarda i destinatari delle comunicazioni, il GEPD preferisce il testo del PE e della Commissione a quello del Consiglio. In effetti il PE ha sostituito la parola «abbonati» con la parola «utenti». La Commissione usa «abbonati» e «singoli interessati». Sia il testo del PE che quello della Commissione includerebbero come destinatari delle comunicazioni non solo gli abbonati ma anche precedenti abbonati e terzi, quali gli utenti che interagiscono con determinati soggetti contemplati senza avere un abbonamento. Il GEPD accoglie favorevolmente questo approccio e invita il PE e il Consiglio a mantenerlo.

59. Tuttavia, il GEPD rileva alcune incoerenze terminologiche nella prima lettura del PE che andrebbero rimosse. Per esempio, la parola «abbonati» è stata sostituita nella maggior parte dei casi, ma non sempre, con la parola «utenti», in altri casi con «consumatori». In questi casi è necessaria un'armonizzazione.

III. **CAMPO DI APPLICAZIONE DELLA DIRETTIVA E-PRIVACY: RETI PUBBLICHE E PRIVATE**

60. L'articolo 3, paragrafo 1 della vigente direttiva e-privacy determina i soggetti principalmente interessati dalla direttiva, ossia coloro che effettuano il trattamento dei dati «*connesso alla*» fornitura di servizi pubblici di comunicazione elettronica su reti pubbliche (sopra indicati come «PPECS») ([15]). Tra gli esempi delle attività dei PPECS figurano la fornitura di accesso a Internet, la trasmissione di informazioni attraverso reti elettroniche, le connessioni telefoniche fisse e mobili, ecc.

61. Il Parlamento europeo ha votato l'emendamento 121 che modifica l'articolo 3 della proposta iniziale della Commissione, in base al quale il campo di applicazione della direttiva e-privacy è stato ampliato al fine di includere «*il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche e private e su reti private accessibili al pubblico nella Comunità, […]*» (art. 3, paragrafo 1 della direttiva e-privacy). Purtroppo il Consiglio e la Commissione hanno avuto difficoltà ad accettare questo emendamento e non hanno pertanto integrato tale approccio nella posizione comune e nella proposta modificata.

Applicazione della direttiva e-privacy alle reti private accessibili al pubblico

62. Per i motivi illustrati in appresso e al fine di contribuire a promuovere un consenso, il GEPD invita a preservare la sostanza dell'emendamento 121. Inoltre, il GEPD suggerisce di includere un emendamento che contribuisca a precisare ulteriormente i tipi di servizi che rientrerebbero nel campo di applicazione ampliato.

([15]) «La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione».

63. Le reti private sono spesso utilizzate per fornire servizi di comunicazione elettronica quali l'accesso a Internet a un numero indeterminato di persone, potenzialmente elevato. Ciò si verifica ad esempio per l'accesso a Internet negli Internet café come pure nei punti Wi-Fi disponibili in alberghi, ristoranti, aeroporti, treni e in altri stabilimenti aperti al pubblico, ove siffatti servizi sono spesso forniti a complemento di altri servizi (bevande, alloggio, ecc.).

64. In tutti i summenzionati casi, un servizio di comunicazione, ad esempio l'accesso a Internet, è messo a disposizione del pubblico non attraverso una rete pubblica bensì attraverso quella che può essere considerata una rete privata, ossia una rete gestita privatamente. Inoltre, sebbene nei casi succitati il servizio di comunicazione sia fornito al pubblico, poiché il tipo di rete utilizzato è privato anziché pubblico, *si può sostenere che* la fornitura di tali servizi non è contemplata dall'intera direttiva e-privacy o almeno da alcuni dei suoi articoli ([16]). Conseguentemente, i diritti fondamentali dei singoli garantiti dalla direttiva e-privacy non sono protetti in tali casi e si crea una situazione giuridica di squilibrio tra gli utenti che accedono ai medesimi servizi Internet attraverso mezzi di telecomunicazione pubblici e gli utenti che vi accedono attraverso mezzi di telecomunicazione privati. Ciò si verifica nonostante il livello di rischio per la tutela della vita privata e dei dati personali in tutti questi casi sia pari a quello connesso all'utilizzo di reti pubbliche per la trasmissione del servizio. In sintesi, non sembra esistere una giustificazione *razionale* per un trattamento differenziato, ai sensi della direttiva, dei servizi di comunicazione forniti tramite una rete privata rispetto a quelli forniti tramite una rete pubblica.

65. Pertanto il GEPD sarebbe favorevole ad un emendamento, quale l'emendamento 121 del PE, secondo cui la direttiva e-privacy si applicherebbe parimenti al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione *private*.

66. Il GEPD riconosce tuttavia che una siffatta formulazione potrebbe comportare conseguenze imprevedibili ed eventualmente non volute. In realtà, il semplice riferimento alle reti private potrebbe essere interpretato come tale da contemplare situazioni che chiaramente non si intende

([16]) *A contrario*, si potrebbe sostenere che, poiché il servizio di comunicazione è fornito al pubblico, anche se la rete è privata, la fornitura di tali servizi è contemplata dal quadro giuridico esistente malgrado il fatto che la rete sia privata. In realtà, ad esempio, in Francia i datori di lavoro che forniscono ai loro impiegati un accesso a Internet sono stati considerati soggetti equivalenti ai fornitori di servizi Internet che offrono un accesso a Internet su base commerciale. Tale interpretazione non è ampiamente accettata.

contemplare nella direttiva. Ad esempio, si potrebbe affermare che un'interpretazione letterale o rigorosa di tale formulazione potrebbe far rientrare nel campo di applicazione della direttiva i proprietari di case dotate di tecnologia Wi-Fi ([17]), che consente la connessione a chiunque si trovi entro il suo raggio d'azione (che comprende solitamente la casa), benché non sia questo il proposito dell'emendamento 121. Al fine di evitare tale risultato, il GEPD suggerisce di riformulare l'emendamento 121 facendo rientrare nel campo di applicazione della direttiva e-privacy «*il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche o private accessibili al pubblico nella Comunità,…*».

67. Ciò contribuirebbe a chiarire che solo le reti private accessibili al pubblico sarebbero contemplate dalla direttiva e-privacy. Applicando le disposizioni della direttiva e-privacy *unicamente* alle *reti private accessibili al pubblico* (e non a tutte le reti private) si stabilisce un limite, di modo che la direttiva contempli soltanto i servizi di comunicazione forniti su reti private che sono intenzionalmente resi *accessibili* al pubblico. Tale formulazione contribuirà a sottolineare ulteriormente che *la disponibilità* delle reti private *per i membri del grande pubblico* costituisce il fattore essenziale per determinare se queste ultime sarebbero contemplate dalla direttiva (oltre alla fornitura di un servizio di comunicazione accessibile al pubblico). In altri termini, a prescindere dal fatto che la rete sia pubblica o privata, se la rete è intenzionalmente resa disponibile al pubblico al fine di fornire un servizio pubblico di comunicazione, quale l'accesso a Internet, anche se tale servizio è complementare a un altro servizio (ad es. la sistemazione alberghiera), questo tipo di servizio/rete rientrerà nel campo di applicazione della direttiva e-privacy.

68. Il GEPD rileva che l'approccio sopra caldeggiato, secondo il quale le disposizioni della direttiva e-privacy si applicano alle *reti private accessibili al pubblico*, è coerente con le impostazioni adottate in diversi Stati membri, le cui autorità hanno già considerato che tale tipo di servizi come pure i servizi forniti su reti esclusivamente private rientrino nel campo di applicazione delle disposizioni nazionali di attuazione della direttiva e-privacy ([18]).

69. Ai fini di una maggiore certezza del diritto in merito ai soggetti rientranti nel nuovo campo di applicazione, potrebbe essere utile includere nella direttiva e-privacy una modifica che definisca le «reti private accessibili al pubblico», del seguente tenore: «*"rete privata accessibile al pubblico": una rete gestita privatamente alla quale i membri del grande pubblico hanno di norma accesso senza restrizioni, a pagamento o gratuitamente o in connessione con altri servizi o offerte, fatta salva l'accettazione delle condizioni e modalità applicabili.*»

70. In pratica, secondo l'approccio sopra indicato le reti private negli alberghi ed altri stabilimenti che forniscono l'accesso a Internet al grande pubblico tramite una rete privata rientrerebbero nel campo di applicazione. Per contro, la fornitura di servizi di comunicazione su reti esclusivamente private, ove il servizio è limitato a un gruppo ristretto di persone identificabili, non sarebbe contemplata. Pertanto, ad esempio, le reti private virtuali e le case di consumatori dotate di tecnologia Wi-Fi non sarebbero contemplate dalla direttiva. Neppure i servizi forniti tramite reti esclusivamente d'impresa sarebbero contemplati.

Reti private rientranti nel campo di applicazione della direttiva e-privacy

71. L'esclusione delle reti private in quanto tali sopra suggerita dovrebbe essere considerata una misura provvisoria, da discutere ulteriormente. In realtà, in considerazione, da un lato, delle implicazioni in materia di tutela della vita privata derivanti dall'esclusione delle reti puramente private e, d'altro lato, del fatto che tale esclusione interessa un gran numero di persone che accedono abitualmente ad Internet tramite reti d'impresa, tale questione dovrà forse essere riesaminata in futuro. Per questo motivo, e al fine di incentivare il dibattito su tale argomento, il GEPD raccomanda di includere nella direttiva e-privacy un considerando secondo cui la Commissione effettuerà una consultazione pubblica sull'applicazione della direttiva e-privacy a tutte le reti private, con il contributo del GEPD, delle autorità preposte alla protezione dei dati e di altri pertinenti soggetti interessati. Inoltre, il considerando potrebbe precisare che, a seguito della consultazione pubblica, la Commissione dovrebbe presentare proposte appropriate per estendere o limitare i tipi di soggetti che dovrebbe essere contemplati dalla direttiva e-privacy.

72. A complemento di quanto sopra indicato, i diversi articoli della direttiva e-privacy dovrebbero essere modificati di conseguenza, di modo che tutte le disposizioni operative menzionino esplicitamente le reti private disponibili al pubblico oltre alle reti pubbliche.

IV. **TRATTAMENTO DEI DATI RELATIVI AL TRAFFICO A FINI DI SICUREZZA**

73. Durante l'iter legislativo relativo al riesame della direttiva e-privacy, le società fornitrici di servizi di sicurezza hanno ribadito la necessità di introdurre nella suddetta direttiva una disposizione intesa a legittimare la raccolta di dati relativi al traffico al fine di garantire un'effettiva sicurezza in linea.

([17]) Typically wireless Local Area Networks (reti locali tipicamente senza fili) (LAN).

([18]) Cfr. nota a piè di pagina 16.

74. Di conseguenza, il PE ha introdotto l'emendamento 181, che ha creato un nuovo articolo 6, paragrafo 6 bis, che autorizza esplicitamente il trattamento di dati relativi al traffico a fini di sicurezza: «*Senza pregiudizio per il rispetto delle disposizioni diverse dall'articolo 7 della direttiva 95/46/CE e dall'articolo 5 della presente direttiva, i dati possono essere trattati per il legittimo interesse del responsabile del trattamento al fine di applicare misure tecniche intese a garantire la sicurezza della rete e dell'informazione, quali definiti all'articolo 4, lettera c) del regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, di un servizio pubblico di comunicazione elettronica, una rete pubblica o privata di comunicazioni elettroniche, un servizio della società dell'informazione o relativo terminal e dispositivo elettronico di comunicazione, salvo ove su tali interessi prevalgano gli interessi per i diritti e le libertà fondamentali della persona interessata. Tale trattamento deve limitarsi allo stretto necessario ai fini di tale attività di sicurezza.*»

75. La Commissione, nella sua proposta modificata, ha accettato tale emendamento in linea di principio ma, eliminando la clausola che recita: «*Senza pregiudizio […] della presente direttiva*», ha eliminato una clausola fondamentale, intesa ad assicurare il rispetto delle altre disposizioni della direttiva. Il Consiglio ha adottato una versione riformulata, che si è spinta ancora oltre nell'affievolire gli importanti elementi di protezione e di equilibrio degli interessi che erano parte integrante dell'emendamento 181, adottando la seguente formulazione: «*I dati relativi al traffico possono essere trattati nella misura strettamente necessaria […] ai fini della sicurezza delle reti e dell'informazione, quale definita all'articolo 4, lettera c) del regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione*».

76. Come ulteriormente precisato in appresso, l'articolo 6, paragrafo 6 bis è superfluo e soggetto al rischio di abuso, in particolare se adottato in una formulazione che non includa le importanti garanzie, le clausole che assicurino il rispetto delle altre disposizioni della direttiva e l'equilibrio degli interessi. Pertanto il GEPD raccomanda di respingere tale articolo o quanto meno di provvedere a che qualsiasi articolo siffatto in materia comprenda i tipi di garanzie inclusi nell'emendamento 181 adottato dal PE.

Motivazioni giuridiche del trattamento dei dati relativi al traffico applicabili ai servizi di comunicazione elettronica e ad altri responsabili del trattamento ai sensi della vigente normativa sulla protezione dei dati

77. La misura in cui i fornitori di servizi di comunicazione elettronica accessibili al pubblico possono legalmente trattare i dati relativi al traffico è disciplinata a norma dell'articolo 6 della direttiva e-privacy, che limita il trattamento dei dati relativi al traffico ad una serie circoscritta di finalità quali la fatturazione, l'interconnessione e la commercializzazione. Tale trattamento può aver luogo soltanto fatte salve determinate condizioni, quali il consenso delle persone interessate nel caso della commercializzazione. Inoltre, altri responsabili del trattamento quali i fornitori di servizi della società dell'informazione possono trattare i dati relativi al traffico a norma dell'articolo 7 della direttiva sulla tutela dei dati, che stabilisce che i responsabili del trattamento possono effettuare il trattamento di dati personali se soddisfano almeno una delle basi giuridiche elencate, menzionate anche come motivazioni giuridiche.

78. Un esempio di siffatte basi giuridiche è costituito dall'articolo 7, lettera a), della direttiva sulla tutela dei dati, che richiede il consenso della persona interessata. Ad esempio, se un rivenditore in linea intende trattare dati relativi al traffico al fine di pubblicizzare o commercializzare del materiale, deve ottenere il consenso della persona interessata. Un'altra base giuridica stabilita all'articolo 7 può consentire, in taluni casi, il trattamento di dati relativi al traffico a fini di sicurezza, ad esempio da parte delle società di sicurezza che forniscono servizi di sicurezza. Tale facoltà si basa sull'articolo 7, lettera f), che stabilisce che i responsabili del trattamento possono effettuare il trattamento di dati personali se ciò è «*necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata …*». La direttiva sulla tutela dei dati non specifica i casi in cui il trattamento di dati personali sarebbe tale da soddisfare detto requisito. Per contro, le decisioni sono adottate dai responsabili del trattamento, caso per caso, spesso con l'accordo delle autorità nazionali preposte alla protezione dei dati e di altre autorità.

79. Si dovrebbe esaminare l'interazione tra l'articolo 7 della direttiva sulla tutela dei dati e il proposto articolo 6, paragrafo 6 bis della direttiva e-privacy. Il proposto articolo 6, paragrafo 6 bis specifica le circostanze in cui i requisiti dell'articolo 7, lettera f) di cui sopra sarebbero soddisfatti. In effetti, autorizzando il trattamento di dati relativi al traffico al fine di contribuire a garantire la sicurezza delle reti e delle informazioni, l'articolo 6, paragrafo 6 bis autorizza tale trattamento per il perseguimento dell'interesse legittimo del responsabile del trattamento.

80. Come ulteriormente precisato in appresso, il GEPD ritiene che il proposto articolo 6, paragrafo 6 bis non sia né necessario né utile. In effetti, dal punto di vista giuridico, è in linea di principio superfluo stabilire se un particolare tipo di attività di trattamento di dati, nella fattispecie il trattamento di dati relativi al traffico a fini di sicurezza, soddisfi o meno i requisiti di cui all'articolo 7, lettera f) della direttiva sulla tutela dei dati, nel qual caso può essere necessario il consenso della persona interessata ai sensi dell'articolo 7, lettera a). Come sopra rilevato, tale valutazione è solitamente effettuata dai responsabili del trattamento, ossia le società, in sede di attuazione, in consultazione con le autorità preposte alla protezione dei dati e, ove necessario, dagli organi giurisdizionali. In generale, il

GEPD ritiene probabile che, in casi specifici, il legittimo trattamento dei dati relativi al traffico a fini di sicurezza, effettuato senza pregiudicare i diritti e le libertà fondamentali delle persone, soddisfi i requisiti di cui all'articolo 7, lettera f) della direttiva sulla tutela dei dati e possa pertanto essere effettuato. Inoltre, non esistono precedenti nell'ambito della direttiva sulla tutela dei dati e della direttiva e-privacy per operare una distinzione o riservare un trattamento speciale a determinati tipi di attività di trattamento di dati che soddisferebbero i requisiti di cui all'articolo 7, lettera f), e non è stata dimostrata la necessità di una siffatta eccezione. Per contro, come sopra rilevato, risulta che in numerosi casi questo tipo di attività sarebbe ampiamente in linea con il testo attuale. Pertanto una disposizione giuridica che confermi tale valutazione è in linea di principio superflua.

Formulazioni dell'articolo 6, paragrafo 6 bis elaborate dal PE, dal Consiglio e dalla Commissione

81. Come sopra precisato, è importante sottolineare che, benché superfluo, l'emendamento 181 quale adottato dal PE è stato nondimeno redatto, tenendo conto in certa misura dei principi relativi alla vita privata e alla protezione dei dati sanciti nella legislazione sulla protezione dei dati. L'emendamento 181 del PE avrebbe potuto tener maggiormente conto delle preoccupazioni concernenti la protezione dei dati e la vita privata, ad esempio inserendo l'espressione «in casi specifici» al fine di assicurare l'applicazione selettiva dell'articolo in questione o prevedendo un periodo specifico di conservazione.

82. L'emendamento 181 contiene alcuni elementi positivi. Esso conferma che il trattamento dovrebbe ottemperare ad ogni altro principio in materia di protezione dei dati applicabile al trattamento dei dati personali («*Senza pregiudizio per il rispetto delle disposizioni […] della direttiva 95/46/CE e […] della presente direttiva*»). Inoltre l'emendamento 181, benché autorizzi il trattamento dei dati relativi al traffico a fini di sicurezza, raggiunge un equilibrio tra gli interessi del soggetto che effettua il trattamento dei dati relativi al traffico e quelli delle persone i cui dati sono oggetto di trattamento, cosicché tale trattamento di dati può aver luogo soltanto se gli interessi del soggetto che effettua il trattamento dei dati non prevalgono sugli interessi per i diritti e le libertà fondamentali della persona interessata («*salvo ove su tali interessi prevalgano gli interessi per i diritti e le libertà fondamentali della persona interessata*»). Tale requisito è essenziale in quanto può permettere il trattamento dei dati relativi al traffico in casi specifici, ma non consentirebbe ad un soggetto di effettuare il trattamento dei dati relativi al traffico alla rinfusa.

83. La versione dell'emendamento riformulata dal Consiglio contiene elementi apprezzabili, quali l'inserimento dei termini «*strettamente necessaria*», che sottolineano il campo di applicazione limitato dell'articolo in questione. Tuttavia, la versione del Consiglio elimina le garanzie concernenti la protezione dei dati e la vita privata sopra menzionate. Sebbene in linea di principio si applichino le disposizioni generali in materia di protezione dei dati, a prescindere dalla presenza di un riferimento specifico in ogni singolo caso, la versione dell'articolo 6, paragrafo 6 bis formulata dal Consiglio può nondimeno essere interpretata come tale da conferire pieno potere discrezionale di effettuare il trattamento dei dati relativi al traffico senza essere soggetti alle garanzie concernenti la protezione dei dati e la vita privata che si applicano in caso di trattamento di dati relativi al traffico. Si potrebbe pertanto sostenere che i dati relativi al traffico possono essere raccolti, memorizzati e ulteriormente utilizzati senza dover ottemperare ai principi e agli obblighi specifici in materia di protezione dei dati che si applicano altrimenti ai soggetti responsabili, come il principio di qualità o l'obbligo di effettuare un trattamento in modo corretto e lecito e di garantire la riservatezza e la sicurezza dei dati. Inoltre, poiché l'articolo non contiene alcun riferimento ai principi applicabili in materia di protezione dei dati che impongono limiti temporali alla conservazione delle informazioni o a termini specifici, la versione del Consiglio può essere interpretata come tale da consentire la raccolta e il trattamento dei dati relativi al traffico a fini di sicurezza per un periodo indeterminato di tempo.

84. Inoltre, il Consiglio ha indebolito la protezione della vita privata in talune parti del testo estendendo potenzialmente la formulazione. Ad esempio, il riferimento al «*legittimo interesse del responsabile del trattamento*» è stato soppresso, suscitando dubbi in merito ai tipi di soggetti che potrebbero avvalersi di tale eccezione. È estremamente importante evitare di favorire la possibilità che qualsiasi utente o soggetto giuridico tragga vantaggio da tale modifica.

85. Le recenti esperienze nell'ambito del PE e del Consiglio dimostrano che è difficile definire mediante norme giuridiche la misura e le condizioni in cui il trattamento dei dati a fini di sicurezza può essere effettuato legalmente. È improbabile che qualsiasi articolo esistente o futuro elimini gli ovvi rischi di un'applicazione troppo estesa dell'eccezione per motivi diversi da quelli esclusivamente correlati alla sicurezza o da parte di soggetti che non dovrebbero poter beneficiare dell'eccezione. Ciò non significa che tale trattamento non possa aver luogo in ogni caso. Tuttavia, la possibilità di effettuare il trattamento e l'entità di quest'ultimo possono meglio essere valutate a livello di attuazione. I soggetti che intendono intraprendere tale trattamento dovrebbero discuterne la portata e le condizioni con le autorità preposte alla protezione dei dati ed eventualmente con il Gruppo dell'articolo 29. Alternativamente, la direttiva e-privacy potrebbe includere un articolo che autorizzi il trattamento dei dati relativi al traffico a fini di sicurezza, fatta salva l'esplicita autorizzazione delle autorità preposte alla protezione dei dati.

86. Tenendo conto, da un lato, dei rischi che l'articolo 6, paragrafo 6 bis presenta per il diritto fondamentale alla protezione dei dati e alla vita privata delle persone e, d'altro lato, del fatto che, come precisato nel presente parere, dal punto di vista giuridico tale articolo è superfluo, il GEPD è giunto alla conclusione che la migliore soluzione consisterebbe nella completa soppressione del proposto articolo 6, paragrafo 6 bis.

87. Nel caso in cui, in contrasto con la raccomandazione del GEPD, venga adottato un testo sulla falsariga dell'attuale versione dell'articolo 6, paragrafo 6 bis, detto testo dovrebbe comunque contenere le garanzie in materia di protezione dei dati sopra discusse. Esso dovrebbe altresì essere opportunamente integrato nell'attuale struttura dell'articolo 6, preferibilmente come nuovo paragrafo 2 bis.

V. **LA POSSIBILITÀ OFFERTA ALLE PERSONE GIURIDICHE DI PROMUOVERE AZIONI GIUDIZIARIE IN CASO DI VIOLAZIONE DELLA DIRETTIVA E-PRIVACY**

88. Il PE ha votato l'emendamento 133 che offre la possibilità ai fornitori di accesso a Internet ed altre persone giuridiche quali le associazioni di consumatori di promuovere un'azione giudiziaria contro le violazioni di una delle disposizioni della direttiva e-privacy ([19]). Purtroppo, né la Commissione né il Consiglio hanno accettato l'emendamento. Il GEPD ritiene tale emendamento molto positivo e ne raccomanda il mantenimento.

89. Per comprendere l'importanza di detto emendamento, occorre rendersi conto del fatto che, nel settore della protezione della vita privata e dei dati, il danno inflitto ad una persona considerata singolarmente non è generalmente sufficiente di per sé a giustificare la promozione di azioni giudiziarie da parte della persona interessata. Le persone di norma non adiscono un tribunale per conto proprio perché sono state vittime di spam o il loro nome è stato erroneamente inserito in un elenco. L'emendamento in questione consentirebbe alle associazioni di consumatori e ai sindacati che rappresentano gli interessi dei consumatori a livello collettivo di promuovere azioni giudiziarie per loro conto dinanzi a un organo giurisdizionale. Probabilmente, inoltre, una maggiore varietà di meccanismi di controllo favorirebbe un più ampio grado di osservanza e sarebbe pertanto nell'interesse di un'efficace applicazione delle disposizioni della direttiva e-privacy.

90. Esistono precedenti giuridici nei quadri normativi di alcuni Stati membri che prevedono già la possibilità di un'azione collettiva intesa a permettere ai consumatori o ai gruppi di interesse di chiedere un risarcimento alla parte che ha cagionato il danno.

91. Inoltre, il diritto della concorrenza di alcuni Stati membri ([20]) autorizza i consumatori, i gruppi di interesse (oltre al *concorrente leso*) ad adire le vie legali avverso il soggetto responsabile della violazione. La motivazione soggiacente a tale approccio consiste nel fatto che è probabile che le società che agiscono in violazione del diritto della concorrenza ne traggano vantaggio, poiché i consumatori che subiscono solo danni marginali sono di norma riluttanti ad adire le vie legali. Tale motivazione può applicarsi *mutatis mutandis* in materia di protezione dei dati e di vita privata.

92. Elemento più importante, come sopra menzionato, è il fatto che, autorizzando le persone giuridiche quali le associazioni di consumatori e i PPECS ad adire le vie legali, si favorisce la posizione dei consumatori e si promuove la generale osservanza della normativa sulla protezione dei dati. Se le società responsabili di violazioni incorrono in un rischio più elevato di essere oggetto di un'azione giudiziaria, è probabile che investano maggiormente nell'osservanza della normativa sulla protezione dei dati, con conseguente aumento a lungo termine del livello di protezione della vita privata e dei consumatori. Per tutti questi motivi il GEPD invita il PE e il Consiglio ad adottare una disposizione che consenta alle persone giuridiche di promuovere un'azione giudiziaria contro le violazioni di una delle disposizioni della direttiva e-privacy.

([19]) Articolo 13, paragrafo 6 della prima lettura del PE.

([20]) Si veda, ad esempio, il paragrafo 8 della legge tedesca contro la concorrenza sleale (LCSI).

VI. **CONCLUSIONI**

93. La posizione comune del Consiglio, la prima lettura del PE e la proposta modificata della Commissione contengono, in diversa misura, elementi positivi che servirebbero a rafforzare la protezione della vita privata e dei dati personali.

94. Tuttavia, il GEPD ritiene che vi sia un margine di miglioramento, in particolare per quanto riguarda la posizione comune del Consiglio che, purtroppo, non ha mantenuto alcuni degli emendamenti del PE intesi a contribuire ad assicurare un'adeguata protezione della vita privata e dei dati personali. Il GEPD esorta il PE e il Consiglio a ripristinare le garanzie in materia di vita privata incorporate nella prima lettura del PE.

95. Inoltre, il GEPD ritiene sia opportuno procedere ad una semplificazione di alcune disposizioni della direttiva. Ciò vale in particolare nel caso delle disposizioni in materia di violazioni di sicurezza, in quanto il GEPD ritiene che i vantaggi della notificazione di violazione si concretizzeranno in maniera ottimale se il quadro giuridico è stabilito correttamente sin dall'inizio. Infine, il GEPD ritiene sia opportuno migliorare e chiarire la formulazione di alcune disposizioni della direttiva.

96. Alla luce di quanto precede, il GEPD esorta il PE e il Consiglio ad intensificare gli sforzi al fine di migliorare e chiarire alcune disposizioni della direttiva e-privacy, ripristinando nel contempo gli emendamenti adottati dal PE in prima lettura e volti a garantire un livello appropriato di protezione della vita privata e dei dati. A tal fine, nei successivi punti 97, 98, 99 e 100 sono sintetizzate le problematiche in questione e sono formulate raccomandazioni e proposte redazionali. Il GEPD invita tutte le parti interessate a tenerne conto in quanto la direttiva e-privacy si avvia verso la fase dell'adozione definitiva.

Violazione di sicurezza

97. Il Parlamento europeo, la Commissione e il Consiglio hanno adottato approcci differenti per quanto riguarda la notificazione di violazioni di sicurezza. Le differenze tra i tre modelli riguardano segnatamente i soggetti contemplati dall'obbligo, il criterio o l'elemento di attivazione della notificazione, gli interessati autorizzati a ricevere la notificazione, ecc. È necessario che il PE e il Consiglio facciano tutto il possibile per produrre un quadro giuridico solido per quanto riguarda la violazione di sicurezza. A tal fine, il PE e il Consiglio dovrebbero:

— *mantenere* la definizione di violazione di sicurezza nei testi del PE, del Consiglio e della Commissione, in quanto essa è abbastanza generale per abbracciare la maggior parte delle pertinenti situazioni in cui la notificazione di violazioni di sicurezza potrebbe essere giustificata;

— per quanto riguarda la portata dei soggetti cui si deve applicare il proposto obbligo di notificazione, *includere* i fornitori di servizi della società dell'informazione. Anche i rivenditori in linea, le banche in linea e le farmacie in linea possono subire violazioni di sicurezza alla stessa stregua delle società di telecomunicazione, se non in misura maggiore. I cittadini si attenderanno di ricevere una notificazione non soltanto quando i fornitori dell'accesso a Internet subiscono violazioni di sicurezza ma in particolare quando ciò accade alle loro banche in linea e farmacie in linea.

— Per quanto riguarda l'attivazione della notificazione, il criterio previsto dalla proposta modificata «*ragionevolmente probabile che possa ledere*» è un criterio appropriato che assicura la funzionalità del sistema. Tuttavia, è importante far sì che il concetto di «ledere» sia sufficientemente ampio da contemplare tutte le pertinenti fattispecie di effetti negativi sulla vita privata o su altri interessi legittimi delle persone. Altrimenti, sarebbe preferibile introdurre un nuovo criterio in base al quale la notificazione sarebbe obbligatoria «*se vi è una probabilità ragionevole che la violazione produca effetti negativi per le persone*». L'approccio del Consiglio, secondo cui la violazione deve pregiudicare *gravemente* la vita privata di una persona, fornirebbe una protezione inadeguata ai singoli nella misura in cui tale criterio richiede che l'effetto sulla vita privata sia «grave». Ciò dà altresì adito a una valutazione soggettiva.

— Benché il coinvolgimento di un'autorità nel determinare se un soggetto interessato debba effettuare la notificazione alle persone abbia certamente effetti positivi, può risultare di difficile realizzazione e applicazione e può inoltre sottrarre risorse ad altre importanti priorità. Se le autorità non possono reagire con estrema rapidità, il GEPD teme che tale sistema possa perfino ridurre la protezione delle persone ed esercitare un'indebita pressione sulle autorità. Quindi, tutto considerato, il GEPD consiglia di *creare* un sistema in cui competa ai soggetti interessati valutare se essi debbano procedere alla notificazione.

— Al fine di consentire alle autorità di esercitare una supervisione sulle valutazioni effettuate dai soggetti contemplati in merito all'opportunità di effettuare una notificazione, il PE e il Consiglio dovrebbero *porre in atto* le garanzie seguenti:

  — *provvedere* affinché tali soggetti siano obbligati a notificare alle autorità tutte le violazioni che soddisfano il criterio prescritto;

  — *affidare* alle autorità un ruolo di supervisione, che consenta loro di essere selettive per poter essere efficaci. A tal fine, occorre aggiungere il seguente testo: «*Se l'abbonato o il singolo interessato non ha ancora ricevuto la notificazione, le autorità nazionali competenti, considerata la natura della violazione, possono chiedere ai PPECS o agli ISSP di provvedere alla notificazione*»;

  — *adottare* una nuova disposizione che prescriva ai soggetti interessati di mantenere piste di controllo interno dettagliate e globali. Ciò potrebbe essere conseguito con l'adozione del seguente testo: «*I PPECS e gli ISSP effettuano e conservano una registrazione completa e dettagliata di tutte le violazioni di sicurezza occorse, delle pertinenti informazioni tecniche ad esse correlate e delle misure adottate per porvi rimedio. I registri contengono altresì un riferimento a tutte le notificazioni effettuate agli abbonati o ai singoli interessati nonché alle autorità nazionali competenti, inclusi le relative date e il relativo contenuto. I registri sono prodotti all'autorità nazionale competente a sua richiesta*».

— Al fine di assicurare la coerenza nell'attuazione del quadro relativo alla violazione di sicurezza, il PE e il Consiglio dovrebbero *attribuire* alla Commissione la facoltà di adottare misure tecniche di attuazione, previa consultazione del GEPD, del Gruppo dell'articolo 29 e di altri pertinenti soggetti interessati.

— Per quanto riguarda i singoli cui deve essere effettuata la notificazione, si dovrebbero *utilizzare* i termini della Commissione o del PE «singoli interessati» o «utenti interessati» in quanto includono tutte le persone i cui dati personali sono stati compromessi.

Reti private accessibili al pubblico

98. I servizi di comunicazione sono spesso messi a disposizione del pubblico non attraverso reti pubbliche bensì attraverso reti gestite privatamente (ad es. punti Wi-Fi disponibili in alberghi e aeroporti), presumibilmente non contemplate dalla direttiva. Il PE ha adottato l'emendamento 121 (articolo 3) che amplia il campo di applicazione della direttiva per includervi le reti di comunicazione pubbliche e private nonché le reti private accessibili al pubblico. A tal fine, il PE e il Consiglio dovrebbero:

— *mantenere* la sostanza dell'emendamento 121, ma *riformularlo* facendo rientrare nel campo di applicazione della direttiva e-privacy «*il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche o private accessibili al pubblico nella Comunità*». Le reti gestite a livello esclusivamente privato (a differenza delle reti private accessibili al pubblico) non sarebbero espressamente contemplate;

— *modificare* di conseguenza tutte le disposizioni operative per menzionare esplicitamente le reti private accessibili al pubblico oltre alle reti pubbliche;

— *includere* una modifica contenente la seguente definizione: «*"rete privata accessibile al pubblico": una rete gestita privatamente alla quale i membri del grande pubblico hanno di norma accesso senza restrizioni, a pagamento o gratuitamente o in connessione con altri servizi o offerte, fatta salva l'accettazione delle condizioni e modalità applicabili*». Ciò assicurerà una maggiore certezza del diritto per quanto riguarda i soggetti rientranti nel nuovo campo di applicazione;

— *adottare* un nuovo considerando, secondo cui la Commissione dovrebbe effettuare una consultazione pubblica sull'applicazione della direttiva e-privacy a tutte le reti private, con il contributo del GEPD, del Gruppo dell'articolo 29 e di altri pertinenti soggetti interessati. Occorrerebbe precisare che, a seguito della consultazione pubblica, la Commissione dovrebbe presentare proposte appropriate per estendere o limitare i tipi di soggetti che dovrebbero essere contemplati dalla direttiva e-privacy.

Trattamento dei dati relativi al traffico a fini di sicurezza

99. Il PE ha adottato in prima lettura l'emendamento 181 (articolo 6, paragrafo 6 bis), che autorizza il trattamento dei dati relativi al traffico a fini di sicurezza. Il Consiglio, nella sua posizione comune, ha adottato una nuova versione che affievolisce alcune della garanzie in materia di vita privata. Al riguardo, il GEPD raccomanda che il PE e il Consiglio:

— *respingano* tale articolo nella sua totalità in quanto superfluo e, se oggetto di abuso, tale da poter indebitamente minacciare la protezione dei dati e la vita privata delle persone;

— alternativamente, se dovesse essere adottata una qualche variante dell'articolo 6, paragrafo 6 bis, *incorporino* le garanzie in materia di protezione dei dati discusse nel presente parere (analoghe a quelle previste dall'emendamento del PE).

Azioni giudiziarie in caso di violazione della direttiva e-privacy

100. Il Parlamento ha adottato l'emendamento 133 (articolo 13, paragrafo 6) che attribuisce alle persone giuridiche la facoltà di promuovere un'azione giudiziaria contro le violazioni di una qualsiasi disposizione della direttiva. Purtroppo il Consiglio non ha accolto tale emendamento. Il Consiglio e il PE dovrebbero:

— *approvare* la disposizione che consente alle persone giuridiche, quali le associazioni di consumatori e di categoria, di promuovere azioni giudiziarie in caso di violazione di qualsiasi disposizione della direttiva (non solo in caso di violazione delle disposizioni in materia di spam, secondo l'attuale approccio della posizione comune e della proposta modificata). Una maggiore varietà di meccanismi di controllo favorirà un più ampio grado di osservanza e un'applicazione più efficace delle disposizioni della direttiva e-privacy nel suo insieme.

Raccogliere la sfida

101. In relazione a tutte le summenzionate questioni, il PE e il Consiglio devono raccogliere la sfida dell'elaborazione di norme e disposizioni adeguate, che siano attuabili e funzionali e rispettino il diritto alla protezione dei dati personali e della vita privata delle persone. Il GEPD auspica che le parti interessate facciano tutto il possibile per raccogliere tale sfida e spera che il presente parere contribuisca a tal fine.

Fatto a Bruxelles, il 9 gennaio 2009.

Peter HUSTINX

Garante europeo della protezione dei dati

Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Consiglio che stabilisce l'obbligo per gli Stati membri di mantenere un livello minimo di scorte di petrolio greggio e/o di prodotti petroliferi

(2009/C 128/05)

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 ([1]),

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 ([2]),

vista la richiesta di parere a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 trasmessa al GEPD il 14 novembre 2008,

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE

1. Il 13 novembre 2008 la Commissione ha adottato una proposta di direttiva del Consiglio che stabilisce l'obbligo per gli Stati membri di mantenere un livello minimo di scorte di petrolio greggio e/o di prodotti petroliferi (in prosieguo «la proposta») ([3]).

2. La proposta è intesa ad assicurare un livello elevato di sicurezza dell'approvvigionamento di petrolio nella Comunità, grazie a meccanismi affidabili e trasparenti basati sulla solidarietà tra Stati membri, a mantenere un livello minimo di scorte di petrolio e di prodotti petroliferi oltre che a dispiegare i mezzi procedurali necessari per rimediare a un'eventuale situazione di grave penuria.

3. Il 14 novembre 2008 la proposta è stata trasmessa dalla Commissione al GEPD per consultazione, a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001. Il GEPD si compiace di essere stato consultato sulla questione e prende atto del riferimento a tale consultazione che figura nel preambolo della proposta, in conformità dell'articolo 28 del regolamento (CE) n. 45/2001.

4. Prima dell'adozione della proposta, la Commissione ha consultato in maniera informale il GEPD su uno specifico articolo del progetto di proposta (l'attuale articolo 19); il GEPD se ne è compiaciuto poiché ha avuto così modo di formulare suggerimenti prima dell'adozione della proposta da parte della Commissione.

II. ANALISI DELLA PROPOSTA

Analisi generale

5. La questione in esame è un buon esempio della necessità di tenere costantemente presenti le norme sulla protezione dei dati. In una situazione che riguarda gli Stati membri e l'obbligo che incombe loro di mantenere scorte di sicurezza di petrolio, detenute per lo più da persone giuridiche, il trattamento dei dati personali non è necessariamente in primo piano; tuttavia, pur non essendo di per sé previsto, può comunque avere luogo. Sarebbe in ogni caso opportuno tenere conto della probabilità che il trattamento di dati personali abbia luogo e agire di conseguenza.

6. Nella versione attuale, la direttiva prevede sostanzialmente due attività che potrebbero comportare il trattamento di dati personali. La prima riguarda la raccolta da parte degli Stati membri di informazioni relative alle scorte petrolifere e il successivo trasferimento di queste informazioni alla Commissione. La seconda riguarda il potere della Commissione di effettuare controlli negli Stati membri. Tra le informazioni da raccogliere riguardo ai proprietari delle scorte petrolifere vi potrebbero essere dati personali, quali nominativi e recapiti dei direttori delle società. La raccolta e il successivo trasferimento alla Commissione di tali informazioni costituirebbero pertanto trattamento di dati personali e renderebbero applicabile la legislazione nazionale che dà attuazione alle disposizioni della direttiva 95/46/CE o alle disposizioni del regolamento (CE) n. 45/2001, a seconda del soggetto che effettua di fatto il trattamento dei dati. Anche il conferimento alla Commissione del potere di effettuare controlli sulle scorte di sicurezza negli Stati membri, che comprende il potere di raccogliere informazioni in generale, potrebbe comportare la raccolta e quindi il trattamento di dati personali.

([1]) GU L 281 del 23.11.1995, pag. 31.
([2]) GU L 8 del 12.1.2001, pag. 1.
([3]) COM(2008) 775 definitivo.

7. Nel corso della consultazione informale, che si è limitata unicamente alla disposizione relativa al potere d'indagine della Commissione, il GEPD ha consigliato alla Commissione di stabilire se il trattamento di dati personali nel contesto di un'indagine condotta dalla Commissione sarebbe solo incidentale oppure se verrebbe effettuato regolarmente e se sarebbe funzionale all'indagine. Sulla scorta dei risultati di questa valutazione sono stati proposti due approcci.

8. Se il trattamento di dati personali non è previsto e sarebbe pertanto puramente incidentale, il GEPD ha raccomandato, in primo luogo, di escludere esplicitamente il trattamento dei dati personali dagli scopi delle indagini della Commissione e, in secondo luogo, di stabilire che i dati personali nei quali la Commissione si dovesse imbattere nel corso delle indagini non sarebbero raccolti né presi in considerazione e, in caso di raccolta accidentale, sarebbero immediatamente distrutti. Come clausola di sicurezza generale, il GEPD suggerisce inoltre di aggiungere una disposizione che stabilisce che la direttiva non pregiudica le norme sulla protezione dei dati di cui alla direttiva 95/46/CE e al regolamento (CE) n. 45/2001.

9. Se, invece, è previsto che il trattamento dei dati avvenga regolarmente nel contesto di un'indagine della Commissione, il GEPD ha raccomandato alla Commissione di inserire un testo che rispecchi il risultato di un'adeguata valutazione in merito alla protezione dei dati. Il testo potrebbe includere i seguenti elementi: I) lo scopo effettivo del trattamento dei dati, II) la necessità del trattamento dei dati per raggiungere tale scopo e III) la proporzionalità del trattamento dei dati.

10. Sebbene il parere informale del GEPD riguardasse soltanto il potere d'indagine della Commissione, le osservazioni del garante si applicano anche all'altra principale attività illustrata nella proposta di direttiva, vale a dire la raccolta e il trasferimento alla Commissione delle informazioni da parte degli Stati membri.

11. La versione definitiva della proposta di direttiva indica chiaramente che la Commissione ha concluso che ai fini della direttiva non è previsto alcun trattamento di dati personali. Il GEPD constata con soddisfazione che la proposta rispecchia pienamente il primo approccio da lui prospettato.

12. Il GEPD sostiene pertanto il modo con cui la Commissione ha assicurato la conformità con le norme sulla protezione dei dati nella proposta di direttiva. Nel seguito del presente parere saranno fornite solo alcune raccomandazioni su aspetti di dettaglio.

Osservazioni su alcuni aspetti di dettaglio

13. L'articolo 15 della proposta di direttiva riguarda l'obbligo per gli Stati membri di trasmettere alla Commissione rilevazioni statistiche settimanali relative al livello delle scorte commerciali detenute sul loro territorio nazionale. Tali informazioni contengono di norma pochi dati di carattere personale. Potrebbero tuttavia contenere ragguagli sulle persone fisiche cui appartengono le scorte petrolifere o che lavorano per una persona giuridica cui appartengono le scorte. Per evitare che gli Stati membri forniscano alla Commissione tali informazioni l'articolo 15, paragrafo 1 stabilisce che, qualora gli Stati membri lo facciano, devono evitare «di menzionare i nominativi dei proprietari delle scorte in questione». Sebbene occorra essere consapevoli del fatto che l'omissione di un nominativo non dà sempre luogo a dati che non possono essere ricollegati a una persona fisica, nella situazione attuale (rilevazioni statistiche dei livelli delle scorte petrolifere) questa frase aggiuntiva sembra essere sufficiente ad assicurare che non avvenga alcun trasferimento di dati personali alla Commissione.

14. Il potere d'indagine della Commissione è stabilito all'articolo 19 della proposta di direttiva. L'articolo indica chiaramente che la Commissione ha seguito il primo approccio illustrato nel precedente punto 8. Secondo tale articolo gli obiettivi dei controlli effettuati dalla Commissione non contemplano la raccolta di dati personali. E, anche se la Commissione si imbattesse in tali dati, questi non potrebbero essere presi in considerazione e, in caso di raccolta accidentale, dovrebbero essere distrutti. Per allineare la formulazione con quella utilizzata nella legislazione in materia di protezione dei dati e al fine di evitare qualunque malinteso, il GEPD raccomanda di sostituire i termini «la raccolta» nella prima frase del paragrafo 2 con i termini «il trattamento».

15. Il GEPD constata con soddisfazione che la proposta comprende anche una clausola di sicurezza generale sulla pertinente legislazione in materia di protezione dei dati. L'articolo 20 ricorda agli Stati membri così come alla Commissione e agli altri organismi comunitari gli obblighi che incombono loro rispettivamente in virtù della direttiva 95/46/CE e del regolamento (CE) n. 45/2001. Nell'articolo si sottolineano altresì i diritti che queste norme conferiscono agli interessati, come il diritto a opporsi al trattamento dei dati che li riguardano, il diritto di accesso a tali dati e il diritto di far rettificare tali dati in caso di inesattezza. Si potrebbe forse formulare un'osservazione sul posizionamento di tale disposizione nella proposta. Trattandosi di una disposizione di carattere generale, non è limitata unicamente al potere d'indagine della Commissione. Il GEPD raccomanda pertanto di spostare l'articolo, collocandolo nella prima parte della direttiva, per esempio dopo l'articolo 2.

16. Anche il considerando 25 contiene un rimando alla direttiva 95/46/CE e al regolamento (CE) n. 45/2001. L'obiettivo del considerando è tuttavia assai poco chiaro in quanto vi si fa riferimento alla legislazione in materia di protezione dei dati unicamente in quanto tale ma non vi sono ulteriori disposizioni. Il considerando dovrebbe stabilire chiaramente che le disposizioni della direttiva lasciano impregiudicata la legislazione citata. Inoltre, l'ultima frase del considerando sembra sottintendere che la legislazione

in materia di protezione dei dati imponga esplicitamente l'obbligo per i responsabili del trattamento di distruggere immediatamente i dati accidentalmente raccolti. Pur essendo una possibile conseguenza delle norme in questione, tale legislazione non contiene detto obbligo. Secondo un principio generale della protezione dei dati, i dati personali sono conservati per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Se la prima parte del considerando sarà adattata nel modo proposto, l'ultima frase diventa superflua. Il GEPD propone pertanto di sopprimere l'ultima frase del considerando 25.

III. **CONCLUSIONE**

17. Il GEPD sostiene il modo con cui la Commissione ha assicurato la conformità con le norme sulla protezione dei dati nella proposta di direttiva.

18. Con riguardo ad aspetti di dettaglio, il GEPD raccomanda quanto segue:

— di sostituire i termini «la raccolta» nella prima frase dell'articolo 19, paragrafo 2 con i termini «il trattamento»;

— di spostare l'articolo 20, che rappresenta la disposizione generale in materia di protezione dei dati, collocandolo nella prima parte della direttiva, e precisamente subito dopo l'articolo 2;

— di aggiungere nel considerando 25 un testo che reciti che le disposizioni della direttiva non pregiudicano le disposizioni della direttiva 95/46/CE e del regolamento (CE) n. 45/2001;

— di sopprimere l'ultima frase del considerando 25.

Fatto a Bruxelles, addì 3 febbraio 2009.

Peter HUSTINX

Garante europeo della protezione dei dati

IV

(Informazioni)

INFORMAZIONI PROVENIENTI DALLE ISTITUZIONI E DAGLI ORGANI DELL'UNIONE EUROPEA

COMMISSIONE

Tassi di cambio dell'euro [1]

5 giugno 2009

(2009/C 128/06)

1 euro =

	Moneta	Tasso di cambio		Moneta	Tasso di cambio
USD	dollari USA	1,4177	AUD	dollari australiani	1,7606
JPY	yen giapponesi	137,48	CAD	dollari canadesi	1,5657
DKK	corone danesi	7,4472	HKD	dollari di Hong Kong	10,9887
GBP	sterline inglesi	0,87920	NZD	dollari neozelandesi	2,2263
SEK	corone svedesi	10,9250	SGD	dollari di Singapore	2,0530
CHF	franchi svizzeri	1,5191	KRW	won sudcoreani	1 768,65
ISK	corone islandesi		ZAR	rand sudafricani	11,4189
NOK	corone norvegesi	8,9700	CNY	renminbi Yuan cinese	9,6871
BGN	lev bulgari	1,9558	HRK	kuna croata	7,3550
CZK	corone ceche	27,003	IDR	rupia indonesiana	14 078,75
EEK	corone estoni	15,6466	MYR	ringgit malese	4,9556
HUF	fiorini ungheresi	289,10	PHP	peso filippino	67,016
LTL	litas lituani	3,4528	RUB	rublo russo	43,5789
LVL	lats lettoni	0,7094	THB	baht thailandese	48,464
PLN	zloty polacchi	4,5420	BRL	real brasiliano	2,7345
RON	leu rumeni	4,2185	MXN	peso messicano	18,7066
TRY	lire turche	2,1834	INR	rupia indiana	66,7910

[1] *Fonte*: tassi di cambio di riferimento pubblicati dalla Banca centrale europea.

RETTIFICHE

Rettifica del tasso di interesse applicato dalla Banca centrale europea alle sue principali operazioni di rifinanziamento

(Gazzetta ufficiale dell'Unione europea C 124 del 4 giugno 2009)

(2009/C 128/07)

A pagina 1 e nel sommario sulla copertina,nel titolo:

anziché: «1,00 % al 4 giugno 2009»,

leggi: «1,00 % al 1º giugno 2009».

PREZZO DEGLI ABBONAMENTI 2009 (IVA esclusa, spese di spedizione ordinaria incluse)

Gazzetta ufficiale dell'UE, serie L + C, unicamente edizione su carta	22 lingue ufficiali dell'UE	1 000 EUR all'anno (*)
Gazzetta ufficiale dell'UE, serie L + C, unicamente edizione su carta	22 lingue ufficiali dell'UE	100 EUR al mese (*)
Gazzetta ufficiale dell'UE, serie L + C, su carta + CD-ROM annuale	22 lingue ufficiali dell'UE	1 200 EUR all'anno
Gazzetta ufficiale dell'UE, serie L, unicamente edizione su carta	22 lingue ufficiali dell'UE	700 EUR all'anno
Gazzetta ufficiale dell'UE, serie L, unicamente edizione su carta	22 lingue ufficiali dell'UE	70 EUR al mese
Gazzetta ufficiale dell'UE, serie C, unicamente edizione su carta	22 lingue ufficiali dell'UE	400 EUR all'anno
Gazzetta ufficiale dell'UE, serie C, unicamente edizione su carta	22 lingue ufficiali dell'UE	40 EUR al mese
Gazzetta ufficiale dell'UE, serie L + C, CD-ROM mensile (cumulativo)	22 lingue ufficiali dell'UE	500 EUR all'anno
Supplemento della Gazzetta ufficiale (serie S — Appalti pubblici), CD-ROM, 2 edizioni la settimana	multilingue: 23 lingue ufficiali dell'UE	360 EUR all'anno (= 30 EUR al mese)
Gazzetta ufficiale dell'UE, serie C — Concorsi	lingua/e del concorso	50 EUR all'anno

(*) Vendita a numero:
- fino a 32 pagine: 6 EUR
- da 33 a 64 pagine: 12 EUR
- oltre 64 pagine: prezzo fissato caso per caso

L'abbonamento alla *Gazzetta ufficiale dell'Unione europea*, pubblicata nelle lingue ufficiali dell'Unione europea, è disponibile in 22 versioni linguistiche. Tale abbonamento comprende le serie L (Legislazione) e C (Comunicazioni e informazioni).

Ogni versione linguistica è oggetto di un abbonamento separato.

A norma del regolamento (CE) n. 920/2005 del Consiglio, pubblicato nella Gazzetta ufficiale L 156 del 18 giugno 2005, in base al quale le istituzioni dell'Unione europea non sono temporaneamente vincolate dall'obbligo di redigere tutti gli atti in lingua irlandese e di pubblicarli in tale lingua, le Gazzette ufficiali pubblicate in lingua irlandese vengono commercializzate separatamente.

L'abbonamento al Supplemento della Gazzetta ufficiale (serie S — Appalti pubblici) riunisce le 23 versioni linguistiche ufficiali in un unico CD-ROM multilingue.

L'abbonamento alla *Gazzetta ufficiale dell'Unione europea* dà diritto a ricevere, su richiesta, i relativi allegati. Gli abbonati sono informati della pubblicazione degli allegati tramite un «Avviso al lettore» inserito nella Gazzetta stessa.

Vendita e abbonamenti

Le pubblicazioni a pagamento dell'Ufficio delle pubblicazioni sono disponibili presso i nostri distributori commerciali. L'elenco dei distributori commerciali è disponibile al seguente indirizzo:

http://publications.europa.eu/others/agents/index_it.htm

EUR-Lex (http://eur-lex.europa.eu) offre un accesso diretto e gratuito al diritto dell'Unione europea. Questo sito consente di consultare la *Gazzetta ufficiale dell'Unione europea* e comprende anche i trattati, la legislazione, la giurisprudenza e gli atti preparatori della legislazione.

Per ulteriori informazioni sull'Unione europea, consultare il sito: http://europa.eu

Ufficio delle pubblicazioni
Publications.europa.eu

UFFICIO DELLE PUBBLICAZIONI UFFICIALI DELLE COMUNITÀ EUROPEE
L-2985 LUSSEMBURGO

IT