Parere del Garante europeo della protezione dei dati — sulla comunicazione della Commissione al Parlamento europeo e al Consiglio — «La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura»

(2011/C 101/02)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

vista la Carta dei diritti fondamentali dell'Unione europea, in particolare gli articoli 7 e 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]),

vista la richiesta di parere a norma del regolamento (CE) n. 45/2001, 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 22 novembre 2010 la Commissione ha adottato una comunicazione dal titolo «La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura» (in prosieguo la «comunicazione») ([3]). La comunicazione è stata trasmessa al GEPD per consultazione.

2. Il GEPD si compiace di essere stato consultato dalla Commissione. Già prima dell'adozione della comunicazione il GEPD aveva formulato osservazioni informali sul progetto di testo, alcune delle quali sono state prese in considerazione nella versione definitiva del documento.

Contesto della comunicazione

3. La strategia di sicurezza interna dell'UE (in prosieguo la SSI), oggetto della comunicazione, era stata adottata il 23 febbraio 2010 sotto la presidenza spagnola ([4]). La strategia definisce un modello di sicurezza europeo che integra, tra l'altro, l'azione della cooperazione tra autorità di contrasto e giudiziarie, la gestione delle frontiere e la protezione civile, nel rispetto dei valori europei comuni, quali i diritti fondamentali. I suoi principali obiettivi sono:

— presentare al pubblico gli strumenti dell'UE esistenti che già contribuiscono a garantire la sicurezza e la libertà dei cittadini dell'UE e il valore aggiunto fornito dall'azione dell'UE in questo settore,

— elaborare ulteriormente strumenti e politiche comuni che utilizzano un approccio più integrato che affronti le cause dell'insicurezza e non soltanto le conseguenze,

— rafforzare la cooperazione tra autorità di contrasto e giudiziarie, la gestione delle frontiere, la protezione civile e la gestione delle catastrofi.

4. La SSI intende far fronte alle minacce e alle sfide più imminenti per la sicurezza dell'Unione europea quali le forme gravi di criminalità organizzata, il terrorismo e la criminalità informatica, la gestione delle frontiere esterne dell'UE e la costruzione della resilienza alle calamità naturali e provocate dall'uomo. La strategia fornisce linee guida, principi e orientamenti generali sul modo in cui l'UE deve affrontare tali questioni e invita la Commissione a proporre azioni programmate per l'attuazione della SSI.

5. A tale proposito è inoltre importante fare riferimento alle recenti conclusioni del Consiglio «Giustizia e affari interni» sull'istituzione e l'attuazione di un ciclo programmatico dell'UE per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale, adottate l'8-9 novembre 2010 ([5]) (in prosieguo le «conclusioni del novembre 2010»). Questo documento fa seguito alle conclusioni del Consiglio sull'architettura della sicurezza interna approvate nel 2006 ([6]) e invita il Consiglio e la Commissione a definire un'ampia strategia di sicurezza interna basata sui valori e i principi comuni dell'UE come ribadito nella Carta dei diritti fondamentali dell'Unione europea ([7]).

([1]) GU L 281 del 23.11.1995, pag. 31.
([2]) GU L 8 del 12.1.2001, pag. 1.
([3]) COM(2010) 673 definitivo.
([4]) Documento del Consiglio 5842/2/10.
([5]) 3043ª sessione del Consiglio «Giustizia e affari interni», 8-10 novembre 2010, Bruxelles.
([6]) Doc. 7039/2/06 GAI 86 CATS 34.
([7]) Il ciclo programmatico dell'UE per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale definito nelle conclusioni del novembre 2010 comporta quattro fasi: 1) sviluppo della politica sulla base di una valutazione da parte dell'Unione europea della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità internazionale (SOCTA dell'UE); 2) definizione e adozione della politica in base all'individuazione, da parte del Consiglio, di un numero limitato di priorità; 3) attuazione e controllo di piani d'azione operativi (OAP) annuali e 4) al termine del ciclo programmatico, svolgimento di una valutazione globale che contribuirà al ciclo programmatico successivo.

6. Tra le linee guida e gli obiettivi che devono orientare l'attuazione della SSI, le conclusioni del novembre 2010 citano l'adozione di un approccio intraprendente e basato sull'intelligence, la stretta cooperazione tra le agenzie dell'Unione, anche sotto il profilo di un ulteriore miglioramento dello scambio di informazioni, e la sensibilizzazione dei cittadini riguardo all'importanza dell'attività svolta dall'Unione per proteggerli. Le conclusioni invitano inoltre la Commissione a elaborare, in collaborazione con gli esperti delle competenti agenzie dell'UE e degli Stati membri, un piano strategico pluriennale (in prosieguo MASP) per ciascuna priorità, in cui sia definita la strategia più opportuna per affrontare il problema. La Commissione è altresì invitata a sviluppare, in consultazione con gli esperti degli Stati membri e delle agenzie dell'UE, un meccanismo indipendente per valutare l'attuazione del MASP e degli OAP. Il GEPD si soffermerà su tali questioni nel prosieguo del presente parere; queste tematiche, infatti, sono strettamente connesse alla protezione dei dati personali, della vita privata e di altri diritti e libertà fondamentali o incidono in maniera significativa su di essa.

Contenuto e obiettivo della comunicazione

7. La comunicazione propone cinque obiettivi strategici, tutti connessi alla tutela della vita privata e alla protezione dei dati:

— smantellare le reti criminali internazionali,

— prevenire il terrorismo e contrastare la radicalizzazione e il reclutamento,

— aumentare i livelli di sicurezza per i cittadini e le imprese nel ciberspazio,

— rafforzare la sicurezza attraverso la gestione delle frontiere, e

— aumentare la resilienza dell'Europa alle crisi e alle calamità.

8. La *strategia di sicurezza interna dell'UE in azione* definita nella comunicazione delinea un programma comune a Stati membri, Parlamento europeo, Commissione, Consiglio, agenzie e altri soggetti, compresi la società civile e le autorità locali, e propone modalità di collaborazione collettiva per i prossimi quattro anni finalizzate al raggiungimento degli obiettivi della SSI.

9. La comunicazione si basa sul trattato di Lisbona e riconosce gli orientamenti forniti dal programma di Stoccolma (e dal relativo piano d'azione), che al capo 4.1 evidenziano la necessità di una SSI globale basata sul rispetto di diritti fondamentali, protezione internazionale e Stato di diritto. Inoltre, ai sensi del programma di Stoccolma, sviluppare, controllare e attuare la strategia di sicurezza interna dovrebbe diventare uno dei compiti prioritari del comitato permanente per la sicurezza interna (COSI) istituito dall'articolo 71 del TFUE. Per assicurare l'effettiva attuazione della SSI, occorre inoltre occuparsi degli aspetti di sicurezza della gestione integrata delle frontiere e, in caso, della cooperazione giudiziaria in materia penale pertinente alla cooperazione operativa nel settore della sicurezza interna. A tale proposito è inoltre importante segnalare che il programma di Stoccolma invita ad adottare un approccio integrato alla SSI che dovrebbe tener conto anche della strategia di sicurezza esterna elaborata dall'Unione nonché di altre politiche dell'UE, in particolare quelle attinenti al mercato interno.

Obiettivo del parere

10. La comunicazione fa riferimento a varie aree politiche che fanno parte di una nozione di «sicurezza interna» nell'Unione europea nella sua ampia accezione o che incidono su di essa.

11. Il presente parere non intende analizzare tutte le aree politiche e le tematiche specifiche contemplate nella comunicazione, bensì:

— esaminare gli obiettivi stessi della SSI proposti nella comunicazione dalla specifica prospettiva della protezione della vita privata e dei dati personali e, da tale angolazione, evidenziare i necessari collegamenti con altre strategie attualmente discusse e adottate a livello UE,

— precisare una serie di nozioni e concetti sulla protezione dei dati che devono essere presi in considerazione nella progettazione, elaborazione e attuazione della SSI a livello UE,

— fornire, se utile e opportuno, suggerimenti sul modo migliore di prendere in considerazione le preoccupazioni in materia di protezione dei dati nell'attuazione delle azioni proposte nella comunicazione.

12. Il GEPD procederà in tal senso evidenziando in particolare i collegamenti tra la SSI e la strategia di gestione delle informazioni e il lavoro sul quadro globale in materia di protezione dei dati. Il GEPD farà altresì riferimento a concetti quali: migliori tecniche disponibili e «privacy by design» (tutela della vita privata fin dalla progettazione), valutazione di impatto sulla tutela della vita privata e sulla protezione dei dati e diritti degli interessati, che hanno un impatto diretto sulla progettazione e attuazione della SSI. Il parere formulerà altresì osservazioni su una serie di aree politiche selezionate quali la gestione integrata delle frontiere, compresi EUROSUR e il trattamento dei dati personali da parte di FRONTEX, nonché altri settori quali il ciberspazio e l'accordo sul programma di controllo delle transazioni finanziarie dei terroristi (TFTP).

II. OSSERVAZIONI GENERALI

La necessità di un approccio più globale, inclusivo e «strategico» alle strategie dell'UE connesse alla SSI

13. A livello UE vengono attualmente discusse e proposte varie strategie dell'Unione europea basate sul trattato di Lisbona e sul programma di Stoccolma e aventi un impatto diretto o indiretto sulla protezione dei dati. La SSI è una di queste ed è strettamente correlata ad altre strategie (affrontate nelle recenti comunicazioni della Commissione o previste nel prossimo futuro) quali la strategia di gestione delle informazioni dell'UE e il modello europeo di scambio delle informazioni, la strategia per il rispetto della Carta dei diritti fondamentali dell'UE, la strategia globale di protezione dei dati e la politica antiterrorismo dell'UE. Nel presente parere il GEPD presta particolare attenzione ai collegamenti con la strategia di gestione delle informazioni e il quadro globale in materia di protezione dei dati basato sull'articolo 16 del TFUE, che presentano le connessioni politiche più evidenti con la SSI dal punto di vista della protezione dei dati.

14. Tutte queste strategie costituiscono un mosaico complesso di programmi, piani d'azione e orientamenti politici interconnessi che richiedono un approccio globale e integrato a livello UE.

15. In termini più generali, se verrà seguito nelle azioni future, questo approccio di «collegamento delle strategie» dimostrerà che a livello UE esiste una visione in materia di strategie dell'Unione europea e che tali strategie e le comunicazioni recentemente adottate su di esse sono di fatto strettamente interconnesse, in quanto il programma di Stoccolma costituisce il punto di riferimento comune a tutte loro. L'adozione di questo approccio determinerà altresì sinergie positive tra le varie politiche riguardanti lo spazio di libertà, sicurezza e giustizia ed eviterà eventuali duplicazioni del lavoro e degli sforzi in questo settore. Aspetto altrettanto importante, da questo approccio scaturirà inoltre un'applicazione più efficace e coerente della normativa in materia di protezione dei dati nel contesto di tutte le strategie interconnesse.

16. Il GEPD sottolinea che uno dei pilastri della SSI è un'efficiente gestione delle informazioni nell'Unione europea che deve fondarsi sui principi di necessità e proporzionalità per giustificare la necessità dello scambio di informazioni.

17. Inoltre, come ha indicato nel parere relativo alla comunicazione della Commissione sulla gestione delle informazioni ([8]), il GEPD sottolinea che tutte le nuove misure legislative volte ad agevolare la conservazione e lo scambio di dati personali devono essere proposte solo qualora la loro necessità sia suffragata da prove concrete ([9]). Questo obbligo giuridico deve tradursi in un approccio politico intraprendente nell'attuazione della SSI. La necessità di adottare un approccio globale alla SSI comporta inevitabilmente la necessità di valutare tutti gli strumenti già esistenti nel settore della sicurezza interna prima di proporne di nuovi.

18. In tale contesto il GEPD suggerisce inoltre un utilizzo più frequente delle clausole che prevedono la valutazione periodica degli strumenti esistenti, conformemente a quanto indicato nella direttiva sulla conservazione dei dati che è attualmente in fase di esame ([10]).

La protezione dei dati quale obiettivo della SSI

19. La comunicazione fa riferimento alla protezione dei dati personali nel paragrafo «Politiche di sicurezza basate su valori comuni», nel quale segnala che gli strumenti e le misure da utilizzare per attuare la SSI devono basarsi su valori comuni fra cui lo Stato di diritto e il rispetto dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea. In tale contesto, stabilisce che «se è vero che lo scambio di informazioni facilita un'efficace attività di contrasto nell'UE, è anche vero che bisogna proteggere la privacy delle persone e il diritto fondamentale alla protezione dei dati personali».

20. Il GEPD accoglie con favore questa affermazione. In quanto tale, tuttavia, non si può ritenere che la questione della protezione dei dati sia tenuta sufficientemente in considerazione nella SSI. La comunicazione non approfondisce la questione della protezione dei dati ([11]) né spiega come il rispetto della vita privata e la protezione dei dati personali saranno garantiti nella pratica nelle azioni per l'attuazione della SSI.

([8]) Parere del 30 settembre 2010 sulla comunicazione della Commissione al Parlamento europeo e al Consiglio — «Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia».

([9]) Questo è un obbligo giuridico; cfr. in particolare la sentenza della Corte nei procedimenti riuniti C-92/09 e C-93/09 del 2 novembre 2010. In contesti più specifici, il GEPD ha sostenuto tale approccio anche in altri pareri su proposte legislative riguardanti lo spazio di libertà, sicurezza e giustizia: ad esempio il parere del 19 ottobre 2005 su tre proposte riguardanti il sistema di informazione Schengen di seconda generazione (SIS II), il parere 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, il parere del 18 febbraio 2009 sulla proposta di regolamento che istituisce l'«Eurodac» per il confronto delle impronte digitali per l'efficace applicazione del regolamento (CE) n. (…/…) (che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide), il parere del 18 febbraio 2009 sulla proposta di regolamento che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e il parere del 7 ottobre 2009 sulle proposte riguardanti l'accesso delle autorità di contrasto all'Eurodac.

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

([11]) La protezione dei dati viene menzionata più specificamente solo nell'ambito della questione del trattamento dei dati personali da parte di FRONTEX.

21. Il GEPD ritiene che tra gli obiettivi della *strategia di sicurezza interna dell'UE in azione* debba figurare il concetto di *protezione* nella sua ampia accezione, grazie a cui verrebbe garantito il *giusto* equilibrio tra, da un lato, la protezione dei cittadini dalle minacce esistenti e, dall'altro, la tutela della loro vita privata e il diritto alla protezione dei dati personali. In altre parole, le preoccupazioni in materia di sicurezza e vita privata devono essere equamente prese in seria considerazione nello sviluppo della SSI, in linea con il programma di Stoccolma e le conclusioni del Consiglio.

22. In sintesi, garantire la sicurezza nel pieno rispetto della vita priva e della protezione dei dati deve essere un vero e proprio obiettivo della strategia di sicurezza interna dell'UE, al quale devono essere improntate tutte le azioni avviate dagli Stati membri e dalle istituzioni dell'Unione europea per l'attuazione della strategia.

23. In tale contesto il GEPD fa riferimento alla comunicazione (2010) 609 su un approccio globale alla protezione dei dati personali nell'Unione europea ([12]). Il GEPD formulerà presto un parere su tale comunicazione, ma in questa sede sottolinea che non è possibile attuare una SSI efficiente senza il sostegno di un solido regime di protezione dei dati che la integri e che fornisca garanzie in termini di fiducia reciproca e

III. NOZIONI E CONCETTI APPLICABILI ALLA PROGETTAZIONE E ALL'ATTUAZIONE DELLA SSI

24. È evidente che alcune delle azioni derivanti dagli obiettivi della SSI possono aumentare i rischi per la vita privata e la protezione dei dati delle persone. Per compensare tali rischi, il GEPD desidera richiamare espressamente l'attenzione su nozioni quali «privacy by design» (tutela della vita privata fin dalla progettazione), valutazione di impatto sulla tutela della vita privata e sulla protezione dei dati, diritti degli interessati e migliori tecniche disponibili (BAT). Tutti questi concetti devono essere presi in considerazione nell'attuazione della SSI e possono fornire un utile contributo alla formulazione di politiche più rispettose della vita privata e orientate alla protezione dei dati in questo settore.

Privacy by design (tutela della vita privata fin dalla progettazione)

25. Il GEPD ha sostenuto in diverse occasioni e in vari pareri il concetto di riservatezza «integrata» [«privacy by design» (tutela della vita privata fin dalla progettazione) o «privacy by default» (riservatezza predefinita)]. Questo concetto viene attualmente sviluppato a livello sia privato che pubblico e pertanto deve svolgere un ruolo importante anche nel contesto della sicurezza interna dell'UE nonché nel settore della polizia e della giustizia ([13]).

26. Questo concetto non viene menzionato nella comunicazione. Il GEPD suggerisce di farvi riferimento nelle azioni mirate da proporre e intraprendere per l'attuazione della SSI, in particolare nel contesto dell'obiettivo 4, «rafforzare la sicurezza attraverso la gestione delle frontiere», in cui viene espressamente indicato un maggiore ricorso alle nuove tecnologie per i controlli di frontiera e la sorveglianza delle frontiere.

Valutazione di impatto sulla tutela della vita privata e sulla protezione dei dati

27. Il GEPD incoraggia la Commissione a riflettere — nell'ambito del lavoro che dovrà essere svolto in futuro riguardo alla progettazione e attuazione della SSI sulla base della comunicazione — su cosa si intenda per una effettiva «valutazione di impatto sulla tutela della vita privata e la protezione dei dati» nello spazio di libertà, sicurezza e giustizia e in particolare nella SSI.

28. Nella comunicazione viene menzionata la valutazione delle minacce e dei rischi. Il GEPD accoglie con favore tale approccio. Il documento, tuttavia, non contiene alcun riferimento alle valutazioni di impatto sulla tutela della vita privata e sulla protezione dei dati. Il GEPD ritiene che il lavoro relativo all'attuazione della comunicazione sulla SSI costituisca una buona occasione per approfondire il concetto di valutazioni di impatto sulla tutela della vita privata e la protezione dei dati nel contesto della sicurezza interna. Il GEPD rileva che né la comunicazione né gli orientamenti per la valutazione d'impatto della Commissione ([14]) specificano questo aspetto e lo traducono in un requisito politico.

29. Il GEPD raccomanda pertanto che nell'attuazione degli strumenti futuri venga effettuata una più specifica e rigorosa valutazione di impatto sulla tutela della vita privata e la protezione dei dati, o come valutazione separata o nell'ambito della valutazione d'impatto generale sui diritti fondamentali svolta dalla Commissione. Tale valutazione d'impatto non deve limitarsi ad affermare principi generali o ad analizzare opzioni politiche, come avviene attualmente, ma deve anche raccomandare garanzie specifiche e concrete.

30. Occorre pertanto definire caratteristiche e indicatori specifici affinché tutte le proposte che incidono sulla tutela della vita privata e sulla protezione dei dati nel settore della sicurezza interna dell'UE siano oggetto di un'analisi approfondita, compresi aspetti quali i principi di proporzionalità, necessità e limitazione delle finalità.

31. In tale contesto, inoltre, potrebbe essere utile fare riferimento all'articolo 4 della raccomandazione RFID ([15]), in cui la Commissione invitava gli Stati membri ad assicurarsi che l'industria, in cooperazione con le parti interessate della

([12]) Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni su un approccio globale alla protezione dei dati nell'Unione europea, COM(2010) 609.

([13]) Il parere del GEPD relativo alla comunicazione della Commissione sul programma di Stoccolma raccomandava di prevedere l'obbligo giuridico per gli ideatori e gli utenti dei sistemi di informazione di sviluppare e utilizzare sistemi conformi al principio della «privacy by design».

([14]) SEC(2009) 92, 15.1.2009.

([15]) COM(2009) 3200 definitivo, 12.5.2009.

società civile, metta a punto un quadro per la realizzazione di valutazioni di impatto sulla tutela della vita privata e la protezione dei dati. Anche la risoluzione di Madrid, adottata nel novembre 2009 dalla conferenza internazionale dei commissari in materia di protezione dei dati e della vita privata, incoraggiava a realizzare valutazioni d'impatto sulla tutela della vita privata e la protezione dei dati prima di attuare nuovi sistemi e tecnologie di informazione per il trattamento di dati personali o di apportare modifiche sostanziali a trattamenti esistenti.

Diritti degli interessati

32. Il GEPD rileva che la comunicazione non prende specificamente in considerazione la questione dei diritti degli interessati, che costituiscono un elemento fondamentale della protezione dei dati e che devono incidere sulla progettazione della SSI. È indispensabile che in tutti i vari sistemi e strumenti relativi alla sicurezza interna dell'UE vengano garantiti alle persone che ne sono oggetto diritti analoghi riguardo alle modalità di trattamento dei loro dati personali.

33. Molti dei sistemi citati nella comunicazione fissano norme specifiche sui diritti degli interessati (riguardanti anche categorie di persone quali vittime, presunti criminali o migranti), ma esistono differenze notevoli tra i diversi sistemi e strumenti, senza una valida giustificazione.

34. Il GEPD invita pertanto la Commissione a esaminare più attentamente la questione dell'allineamento dei diritti degli interessati nell'UE nel contesto della SSI e della strategia di gestione delle informazioni nel prossimo futuro.

35. Occorre prestare una particolare attenzione ai meccanismi di risarcimento. La SSI deve garantire che, nel caso in cui i diritti delle persone non siano stati pienamente rispettati, i responsabili del trattamento dei dati prevedano procedure di reclamo facilmente accessibili, efficaci ed economicamente abbordabili.

Migliori tecniche disponibili

36. L'attuazione della SSI si baserà inevitabilmente sull'utilizzo di un'infrastruttura informatica in grado di supportare le azioni previste nella comunicazione. Le migliori tecniche disponibili (BAT) possono essere considerate come strumenti in grado di garantire il giusto equilibrio tra la realizzazione degli obiettivi della SSI e il rispetto dei diritti delle persone. Nel presente contesto il GEPD desidera ribadire la raccomandazione formulata in precedenti pareri [16] riguardo alla necessità che la Commissione definisca e promuova, insieme alle parti interessate del settore, misure concrete per l'applicazione delle BAT. Per «migliore tecnologia disponibile» si intende la più efficace ed avanzata fase di sviluppo di attività e dei relativi metodi di esercizio, che indicano l'idoneità pratica di determinate tecniche a costituire la base per il conseguimento dei risultati previsti in modo efficiente e nel rispetto del quadro dell'UE sulla tutela della vita privata e sulla protezione dei dati. Questo approccio è pienamente in linea con il concetto di «privacy by design» (tutela della vita privata fin dalla progettazione), precedentemente citato.

37. Laddove sia pertinente e fattibile, occorre elaborare documenti di riferimento sulle BAT volti a fornire orientamenti e a garantire una maggiore certezza del diritto per l'effettiva applicazione delle misure previste nel quadro della SSI. In questo modo si potrebbe inoltre promuovere l'armonizzazione di tali misure in tutti i vari Stati membri. Ultimo ma non meno importante aspetto, la definizione di BAT rispettose della vita privata e della sicurezza agevolerà il ruolo di controllo delle autorità responsabili della protezione dei dati dotandole di riferimenti tecnici, adottati dai responsabili del trattamento dei dati, conformi per quanto riguarda la protezione della vita privata e dei dati.

38. Il GEPD rileva inoltre l'importanza di un corretto allineamento della SSI con le attività già svolte nell'ambito del Settimo programma quadro di ricerca e sviluppo tecnologico e del programma quadro «Sicurezza e tutela delle libertà». Una visione comune finalizzata alla fornitura delle BAT favorirà l'innovazione a livello di conoscenze e capacità necessarie a proteggere i cittadini nel rispetto dei diritti fondamentali.

39. Infine, il GEPD evidenzia il ruolo che può svolgere l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) nell'elaborazione di orientamenti e nella valutazione delle capacità in materia di sicurezza necessarie a garantire l'integrità e la disponibilità dei sistemi informatici nonché nella promozione delle BAT. A tale proposito, il GEPD accoglie con favore l'inclusione dell'agenzia quale attore chiave per il rafforzamento della capacità di far fronte agli attacchi informatici e della lotta contro la criminalità informatica [17].

Precisazione degli attori e dei loro ruoli

40. In questo contesto è inoltre necessario definire con maggiore chiarezza gli attori che fanno parte dell'architettura della SSI o che vi contribuiscono. La comunicazione cita attori e parti interessate differenti quali cittadini, autorità

[16] Parere del GEPD sui sistemi di trasporto intelligenti, del luglio 2009, e parere del GEPD sulla comunicazione RFID del dicembre 2007; cfr. anche la relazione annuale 2006 del GEPD, pagg. 48.

[17] Il GEPD prevede l'adozione di un parere sul quadro giuridico dell'ENISA, ancora nel dicembre 2010.

giudiziarie, agenzie dell'UE, autorità nazionali, polizia e imprese. Le competenze e i ruoli specifici di questi attori devono essere precisati meglio nelle azioni specifiche da proporre per l'attuazione della SSI.

IV. **OSSERVAZIONI SPECIFICHE SU SETTORI POLITICI CONNESSI ALLA SSI**

Gestione integrata delle frontiere

41. La comunicazione fa riferimento al fatto che, con l'entrata in vigore del trattato di Lisbona, l'Unione europea è in grado di trarre maggior vantaggio dalle sinergie fra le politiche di gestione delle frontiere per le persone e le merci. Per quanto riguarda la circolazione delle persone, il documento afferma che «l'UE può guardare alla gestione dell'immigrazione e alla lotta contro la criminalità come a un duplice obiettivo della strategia di gestione integrata delle frontiere». La comunicazione considera la gestione delle frontiere come uno strumento potenzialmente efficace per smantellare le forme gravi di criminalità organizzata ([18]).

42. Il GEPD rileva inoltre che la comunicazione individua tre assi strategici: 1) maggiore ricorso alle nuove tecnologie per i controlli di frontiera (il SIS II, il VIS, il sistema di registrazione ingressi/uscite e il programma per viaggiatori registrati); 2) un maggiore ricorso alle nuove tecnologie per la sorveglianza delle frontiere (sistema europeo di sorveglianza delle frontiere, EUROSUR) e 3) un maggiore coordinamento fra gli Stati membri grazie a FRONTEX.

43. Il GEDP desidera cogliere l'occasione offerta da questo parere per ricordare le richieste, formulate in una serie di pareri precedenti, di definire a livello UE una politica chiara sulla gestione delle frontiere, nel pieno rispetto della normativa in materia di protezione dei dati. Il GEPD ritiene che l'attuale lavoro sulla SSI e la gestione delle informazioni costituisca un'ottima occasione per compiere passi più concreti verso l'adozione di un approccio politico coerente nei confronti di questi settori.

44. Il GEDP rileva che la comunicazione non fa riferimento solo ai sistemi su vasta scala esistenti e a quelli che potrebbero diventare operativi nel prossimo futuro (come il SIS, il SIS II e il VIS), ma — nello stesso paragrafo — cita anche sistemi che potrebbero essere proposti dalla Commissione in futuro ma su cui non è stata ancora presa una decisione (ad esempio il programma per viaggiatori registrati e il sistema di registrazione ingressi/uscite). In tale contesto è necessario ricordare che gli obiettivi e la legittimità dell'introduzione di questi sistemi devono essere ancora chiariti e dimostrati, anche alla luce di valutazioni d'impatto specifiche svolte dalla Commissione. In caso contrario, si può ritenere che la comunicazione anticipi il processo decisionale e di conseguenza non tenga conto del fatto che non è ancora stata presa una decisione definitiva sull'eventuale introduzione nell'Unione europea del programma per viaggiatori registrati e del sistema di registrazione ingressi/uscite.

45. Il GEPD raccomanda pertanto di evitare anticipazioni analoghe nel lavoro futuro sull'attuazione della SSI. Come precedentemente indicato, ogni eventuale decisione sull'introduzione di nuovi sistemi su vasta scala invasivi della vita privata deve essere presa solo a seguito di un'adeguata valutazione di tutti i sistemi esistenti, tenendo nella debita considerazione i principi di necessità e proporzionalità.

EUROSUR

46. La comunicazione riferisce che nel 2011 la Commissione presenterà una proposta legislativa riguardante l'istituzione di EUROSUR per contribuire alla sicurezza interna e alla lotta contro la criminalità. Segnala altresì che EUROSUR si avvarrà delle nuove tecnologie sviluppate grazie ai progetti di ricerca e alle attività finanziate dall'UE, come le immagini satellitari per individuare e seguire obiettivi alle frontiere marittime, ad esempio per tenere sotto controllo imbarcazioni rapide che trasportino droga nell'UE.

47. In tale contesto il GEPD osserva che non è chiaro se, ed eventualmente in quale misura, nella proposta legislativa su EUROSUR che verrà presentata dalla Commissione nel 2011 verrà contemplato il trattamento dei dati personali nell'ambito di EUROSUR. Nella comunicazione la Commissione non ha adottato una posizione chiara sulla questione. Questo aspetto è ancora più rilevante se si considera che la comunicazione collega chiaramente EUROSUR e FRONTEX a livello tattico, operativo e strategico (si vedano le osservazioni formulate di seguito su FRONTEX) e chiede una stretta cooperazione fra di loro.

Il trattamento dei dati personali da parte di FRONTEX

48. Il 17 maggio 2010 il GEPD ha formulato un parere sulla revisione del regolamento FRONTEX ([19]) in cui chiedeva di svolgere un dibattito vero e proprio e una riflessione approfondita sulla questione della protezione dei dati nell'ambito del rafforzamento dei compiti attuali di FRONTEX e del conferimento di nuove responsabilità all'agenzia.

49. La comunicazione segnala la necessità di rafforzare il contributo di FRONTEX alle frontiere esterne nell'ambito dell'obiettivo 4, «rafforzare la sicurezza attraverso la gestione delle frontiere». A tale proposito, la comunicazione afferma che, in base all'esperienza acquisita e nel contesto dell'approccio globale dell'UE alla gestione delle informazioni, la Commissione ritiene che consentire a Frontex di

([18]) Comunicato stampa su «La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura», Memo 10/598.

([19]) Parere del GEPD del 17 maggio 2010 sulla proposta di regolamento del Parlamento europeo e del Consiglio recante modifica del regolamento (CE) n. 2007/2004 del Consiglio che istituisce un'Agenzia europea per la gestione della cooperazione operativa alle frontiere esterne degli Stati membri dell'Unione europea (FRONTEX).

trattare e utilizzare queste informazioni, in misura limitata e conformemente a norme di gestione dei dati personali chiaramente definite, apporterà un contributo significativo allo smantellamento delle organizzazioni criminali. Si tratta di un approccio nuovo rispetto alla proposta della Commissione sulla revisione del regolamento FRONTEX, attualmente oggetto di discussione in seno al Parlamento europeo e al Consiglio, che non si era pronunciato in merito al trattamento dei dati personali.

50. In tale contesto, il GEPD si compiace del fatto che la comunicazione fornisca alcune indicazioni in merito alle circostanze che potrebbero comportare la necessità di procedere al trattamento dei dati (ad esempio analisi dei rischi, operazioni congiunte più mirate o scambio di informazioni con Europol). Più specificamente, la comunicazione spiega che attualmente le informazioni sui criminali appartenenti alle reti di trafficanti — acquisite da FRONTEX — non possono essere successivamente utilizzate ai fini di analisi dei rischi o di future operazioni congiunte più mirate. Per giunta, i dati rilevanti sui presunti criminali non arrivano alle autorità nazionali competenti né ad Europol per ulteriori indagini.

51. Tuttavia, il GEPD osserva che la comunicazione non fa riferimento alla discussione attualmente in corso sulla revisione del quadro giuridico di FRONTEX che, come indicato in precedenza, affronta la questione al fine di fornire soluzioni legislative. Inoltre, la formulazione della comunicazione in cui viene evidenziato il ruolo di FRONTEX nell'ambito dell'obiettivo dello smantellamento delle organizzazioni criminali può essere interpretata come un ampliamento del mandato dell'agenzia. Il GEPD suggerisce di tenere in considerazione questo aspetto sia nella revisione del regolamento FRONTEX che nell'attuazione della SSI.

52. Il GEPD richiama inoltre l'attenzione sulla necessità di garantire l'assenza di duplicazioni fra i compiti di Europol e FRONTEX. A tale proposito, il GEPD si compiace del fatto che la comunicazione indichi la necessità di evitare la creazione di doppioni fra i lavori di FRONTEX ed Europol. Occorre tuttavia affrontare più chiaramente la questione sia nel regolamento FRONTEX rivisto sia nelle azioni per l'attuazione della SSI che prevedono una stretta cooperazione tra FRONTEX ed EUROPOL. Si tratta di un aspetto particolarmente importante dal punto di vista dei principi della limitazione delle finalità e della qualità dei dati. Questa osservazione vale anche per la cooperazione futura con agenzie quali l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) o l'Ufficio europeo di sostegno per l'asilo.

L'utilizzo dei dati biometrici

53. La comunicazione non prende specificamente in considerazione l'attuale fenomeno del crescente utilizzo dei dati biometrici nel settore dello scambio di informazioni nell'UE, compresi i sistemi informatici europei su larga scala e altri strumenti per la gestione delle frontiere.

54. Il GEPD coglie pertanto l'occasione per ricordare il suo suggerimento ([20]) di prendere seriamente in considerazione questo aspetto nell'attuazione della SSI, in particolare nel contesto della gestione delle frontiere, poiché si tratta di una questione di grande sensibilità dal punto di vista della protezione dei dati.

55. Il GEPD raccomanda inoltre di elaborare una politica chiara e rigorosa sull'utilizzo dei dati biometrici nello spazio di libertà, sicurezza e giustizia sulla base di una valutazione seria e ponderando caso per caso la necessità di utilizzare elementi biometrici nell'ambito della SSI, nel pieno rispetto di principi fondamentali per la protezione dei dati quali la proporzionalità, la necessità e la limitazione delle finalità.

TFTP

56. La comunicazione annuncia che nel 2011 la Commissione elaborerà una politica di estrazione e analisi dei dati di messaggistica finanziaria detenuti sul proprio territorio. A tale proposito, il GEPD fa riferimento al parere formulato il 22 giugno 2010 sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP II) ([21]). Tutte le osservazioni critiche espresse in quel parere sono valide e applicabili anche nell'ambito del lavoro previsto su un quadro dell'UE in materia di dati di messaggistica finanziaria. Di conseguenza, devono essere prese in considerazione nelle discussioni sull'argomento. Occorre prestare particolare attenzione alla proporzionalità di estrarre e trattare grandi quantitativi di dati su persone che non sono sospette nonché alla questione di una sorveglianza efficace da parte di autorità indipendenti e autorità giudiziarie.

Sicurezza per i cittadini e le imprese nel ciberspazio

57. Il GEPD accoglie con favore l'importanza attribuita dalla comunicazione alle azioni preventive a livello UE e ritiene che il rafforzamento della sicurezza delle reti informatiche sia un fattore essenziale per il buon funzionamento della società dell'informazione. Il GEPD sostiene inoltre le specifiche attività volte a rafforzare la capacità di far fronte agli attacchi informatici, a potenziare le capacità delle autorità di polizia e degli organi giudiziari e a creare partenariati con l'industria per dare ai cittadini e alle imprese i mezzi per agire. Il GEPD accoglie altresì con favore il ruolo che l'ENISA sarà chiamata a svolgere per spianare la strada a molte delle azioni previste nell'ambito di questo obiettivo.

([20]) Cfr. in particolare il parere del GEPD sulla comunicazione della Commissione sul panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia di cui alla nota a piè di pagina 8.

([21]) Parere del GEPD del 22 giugno 2010 sulla proposta di decisione del Consiglio relativa alla conclusione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP II).

58. Ciononostante, la *strategia di sicurezza interna dell'UE in azione* non illustra le azioni di contrasto previste nel ciberspazio né precisa il modo in cui tali attività potrebbero compromettere i diritti individuali e non indica nemmeno quali dovrebbero essere le garanzie necessarie. Il GEPD chiede di adottare un approccio più ambizioso sulle garanzie adeguate, che dovrà essere definito in modo tale da assicurare la protezione dei diritti fondamentali di tutte le persone, comprese quelle che potrebbero essere interessate da azioni volte a contrastare eventuali attività criminali in questo settore.

V. **CONCLUSIONE E RACCOMANDAZIONI**

59. Il GEPD chiede di collegare le varie strategie e comunicazioni dell'UE nel processo di attuazione della SSI. A questo approccio deve fare seguito un piano d'azione concreto sostenuto da un'effettiva valutazione delle necessità, il cui esito sarà una politica UE globale, integrata e strutturata sulla SSI.

60. Il GEPD coglie inoltre questa occasione per sottolineare l'importanza dell'obbligo giuridico di un'effettiva valutazione di tutti gli strumenti esistenti che devono essere utilizzati nell'ambito della SSI e dello scambio di informazioni prima di proporne di nuovi. A tale proposito, si raccomanda vivamente di includere disposizioni che prevedano valutazioni periodiche dell'efficienza degli strumenti pertinenti.

61. Il GEPD suggerisce di tenere conto, nell'elaborazione del piano strategico pluriennale previsto dalle conclusioni del Consiglio del novembre 2010, del lavoro attualmente in corso sul quadro globale per la protezione dei dati, svolto sulla base dell'articolo 16 del TFUE, in particolare della comunicazione (2009) 609.

62. Il GEPD formula una serie di suggerimenti su nozioni e concetti pertinenti dal punto di vista della protezione dei dati di cui si dovrebbe tenere conto nel settore della SSI, quali «privacy by design» (tutela della vita privata fin dalla progettazione), valutazione di impatto sulla tutela della vita privata e sulla protezione dei dati, migliori tecniche disponibili.

63. Il GEPD raccomanda che nell'attuazione degli strumenti futuri venga effettuata una valutazione di impatto sulla tutela della vita privata e la protezione dei dati, o come valutazione separata o nell'ambito della valutazione d'impatto generale sui diritti fondamentali svolta dalla Commissione.

64. Il GEPD invita inoltre la Commissione a elaborare una politica più coerente e omogenea sui prerequisiti per l'utilizzo dei dati biometrici nell'ambito della SSI e raccomanda un maggiore allineamento dei diritti degli interessati a livello UE.

65. Il GEPD formula infine una serie di osservazioni sul trattamento dei dati personali nell'ambito della gestione delle frontiere e in particolare da parte di FRONTEX nonché, eventualmente, nel contesto di EUROSUR.

Fatto a Bruxelles, il 17 dicembre 2010.

Peter HUSTINX

Garante europeo della protezione dei dati