# GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

## Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di Decisione quadro del Consiglio sullo scambio di informazioni in virtù del principio di disponibilità (COM (2005) 490 defin.)

(2006/C 116/04)

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 richiesta di parere a norma dell'articolo 28, paragrafo 2 del 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,

HA ADOTTATO IL SEGUENTE PARERE:

### I. OSSERVAZIONI PRELIMINARI

1. Con lettera del 12 ottobre 2005 la Commissione ha trasmesso al GEPD la proposta di decisione quadro del Consiglio sullo scambio di informazioni in virtù del principio di disponibilità. Secondo il GEPD la lettera rappresenta una richiesta di fornire alle istituzioni e agli organismi comunitari pareri come previsto nell'articolo 28, paragrafo 2 del regolamento (CE) n. 45/2001. Secondo il GEPD il presente parere dovrebbe essere citato nel preambolo della decisione quadro.

2. La natura del presente parere va vista nel contesto descritto al punto II, in cui si precisa che l'adozione in ultima analisi di uno strumento giuridico in base all'attuale proposta, o all'approccio nei confronti del principio di disponibilità in essa contenuto, non deve essere data per scontata. Un cospicuo numero di Stati membri propende per altri approcci.

3. È evidente tuttavia che la questione della disponibilità di informazioni in materia di applicazione della legge attraverso le frontiere interne o, in senso più ampio, lo scambio di tali informazioni, sia un elemento prioritario all'ordine del giorno degli Stati membri, sia in sede di Consiglio che in altri ambiti, nonché in seno al Parlamento europeo.

4. È parimenti naturale che questa tematica sia fortemente rilevante sotto il profilo della protezione dei dati personali, come il presente parere si appresta ad illustrare. Il GEPD rammenta che l'attuale proposta è stata presentata dalla Commissione in stretta connessione con la proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, che ha formato oggetto di un parere del GEPD presentato il 19 dicembre 2005.

5. Il GEPD coglie l'occasione per illustrare in questo parere alcuni elementi generali e di natura più sostanziale sul tema dello scambio di informazioni in materia di applicazione della legge e sugli approcci per disciplinare questo ambito. Presentando il proprio parere, il GEPD intende fare in modo che la prospettiva della protezione dei dati sia tenuta in debita considerazione in future discussioni sull'argomento.

6. Il GEPD resta disponibile per una nuova consultazione in una fase successiva, quando saranno intervenuti sviluppi nell'iter legislativo della proposta in esame e di altre proposte correlate.

### II. LA PROPOSTA NEL SUO CONTESTO

7. Il principio di disponibilità è stato introdotto come importante nuovo principio di diritto nel programma dell'Aia. In base a detto principio le informazioni necessarie ai fini della lotta contro la criminalità dovrebbero attraversare le frontiere interne dell'UE senza ostacoli. L'obiettivo della proposta è di attuare questo principio in uno strumento giuridico vincolante.

8. Lo scambio di informazioni di polizia tra paesi diversi è materia di discussione abituale tra i legislatori, sia all'interno sia all'esterno dell'UE. Di recente, le seguenti iniziative hanno attirato l'attenzione del GEPD.

9. In primo luogo, il 4 giugno 2004 la Svezia ha presentato una proposta di decisione quadro relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge. Su tale proposta il Consiglio ha convenuto un orientamento generale nella riunione del 1º dicembre 2005.

10. In secondo luogo, il 27 maggio 2005 sette Stati membri hanno firmato a Prüm (Germania) il trattato relativo al rafforzamento della cooperazione transfrontaliera, in particolare per quanto riguarda la lotta al terrorismo, alla criminalità transfrontaliera e all'immigrazione clandestina, che introduce tra l'altro misure volte a migliorare lo scambio di informazioni relative al DNA ed alle impronte digitali. Al trattato può aderire qualsiasi Stato membro dell'Unione europea. Le parti contraenti intendono integrare le disposizioni del trattato nel quadro giuridico dell'Unione europea.

11. In terzo luogo, la disponibilità di informazioni relative all'applicazione della legge attraverso le frontiere interne dell'Unione europea sarà inoltre facilitata ulteriormente grazie ad altri strumenti giuridici, quali le proposte relative al Sistema d'informazione Schengen di seconda generazione (SIS II), la proposta relativa all'accesso per consultazione al sistema d'informazione visti (VIS) e la proposta di decisione quadro relativa all'organizzazione e al contenuto degli scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario. A questo proposito è altresì utile menzionare la comunicazione concernente il miglioramento dell'efficienza e l'incremento dell'interoperabilità e delle sinergie tra banche dati europee nel settore della giustizia e degli affari interni, pubblicata dalla Commissione il 25 novembre 2005.

12. Considerata la molteplicità delle iniziative già avviate, è opportuno non esaminare l'attuale proposta di decisione quadro sulla disponibilità in modo isolato, bensì tener conto anche di altri approcci riguardo allo scambio di informazioni relative all'applicazione della legge. Ciò appare tanto più importante se si considera l'attuale tendenza in sede di Consiglio a preferire altri approcci in materia di scambio di informazioni e di disponibilità rispetto all'approccio generale proposto dalla Commissione nella proposta attuale. L'attuale testo della proposta potrebbe perfino non essere oggetto di discussione in sede di Consiglio.

13. Inoltre la proposta è strettamente connessa alla proposta di decisione quadro sulla protezione dei dati personali. Il presente parere deve essere inteso in connessione con il parere più approfondito relativo a tale decisione quadro.

14. Nel suo parere sulla proposta di decisione quadro relativa alla protezione dei dati personali, il GEPD sottolineava l'importanza di un'adeguata protezione dei dati come necessaria conseguenza di uno strumento giuridico sulla disponibilità. A giudizio del GEPD, tale strumento giuridico non dovrebbe essere adottato senza che siano previste garanzie essenziali in materia di protezione dei dati.

15. Il GEPD assume un'identica posizione riguardo all'adozione di altri strumenti giuridici che facilitino il flusso di informazioni relative all'applicazione della legge attraverso le frontiere interne dell'UE. Il GEPD si compiace pertanto della decisione del Consiglio e del Parlamento europeo di dare priorità alla summenzionata proposta sulla protezione dei dati personali.

## III. IL PRINCIPIO DI DISPONIBILITÀ IN QUANTO TALE

16. Il principio di disponibilità è di per sé un principio semplice. Le informazioni disponibili per talune autorità in uno Stato membro devono essere fornite anche alle autorità omologhe in altri Stati membri. Lo scambio di informazioni tra le autorità degli Stati membri deve avvenire in modo quanto più possibile rapido e semplice, di preferenza accordando l'accesso diretto on line.

17. Le difficoltà hanno origine dal contesto in cui il principio di disponibilità deve essere attuato:

— l'eterogenea organizzazione della polizia e dell'ordinamento giudiziario negli Stati membri, è con freni e contrappesi diversi,

— sono inclusi tipi diversi di informazioni (sensibili), ad esempio il DNA o le impronte digitali,

— le modalità di accesso alle pertinenti informazioni per le autorità competenti sono diverse anche all'interno degli Stati membri,

— è difficile assicurare che le informazioni provenienti da un altro Stato membro siano interpretate correttamente, a causa della diversità delle lingue, dei sistemi tecnologici (interoperabilità) e degli ordinamenti giuridici,

— il principio di disponibilità va inserito nell'ampia varietà delle vigenti disposizioni di legge che riguardano lo scambio di informazioni relative all'applicazione della legge tra paesi.

18. A prescindere dalla complessità del contesto, è comunemente riconosciuto che il principio non può operare autonomamente, ma occorrono misure supplementari per assicurare che le informazioni possano essere effettivamente reperite e consultate. In ogni caso, tali misure devono permettere alle autorità incaricate dell'applicazione della legge di accertare più facilmente se le omologhe autorità di altri Stati membri dispongono di informazioni pertinenti e dove tali informazioni possono essere consultate. Tali misure supplementari potrebbero consistere in interfacce che danno un accesso diretto a tutti i dati o a dati specifici in possesso di altri Stati membri. La proposta di decisione quadro sulla disponibilità introduce per questa ragione la nozione di «dati di indice», ossia dati specifici cui si può accedere direttamente attraverso le frontiere.

19. In generale, il principio di disponibilità dovrebbe facilitare il flusso di informazioni tra gli Stati membri. Le frontiere interne saranno abolite e gli Stati membri devono permettere che le informazioni di cui dispongono le loro autorità di polizia diventino progressivamente accessibili ad altre autorità. Gli Stati membri non sono più competenti a controllare il flusso di informazioni, e di conseguenza non possono più fare affidamento sulla propria legislazione nazionale in quanto strumento sufficiente a garantire una protezione adeguata delle informazioni.

20. Per tale ragione la proposta merita particolare attenzione sotto il profilo della protezione dei dati personali. In primo luogo, le informazioni di regola riservate e protette devono essere fornite alle autorità di altri Stati membri. In secondo luogo, a garanzia del funzionamento del sistema occorre mettere a punto dati di indice e renderli disponibili per le autorità di altri Stati membri. L'attuazione di questo principio darà origine, di conseguenza, ad una mole di dati maggiore rispetto a quelli attualmente disponibili.

## IV. **ELEMENTI PRINCIPALI**

### Ambito di applicazione del principio di disponibilità

21. Innanzitutto è essenziale definire a quale tipo di informazioni si applicherà il principio di disponibilità. L'ambito di applicazione di tale principio è definito in termini generali all'articolo 2 della proposta, in combinato disposto con l'articolo 1, paragrafo 1 e con l'articolo 3, lettera a). Il principio si applica ad informazioni che ottemperano alle seguenti condizioni:

— sono informazioni esistenti,

— figurano nell'elenco di cui all'allegato II, che definisce sei tipi di informazioni,

— sono informazioni di cui dispongono le autorità competenti.

Sono questi i tre elementi essenziali dell'ambito di applicazione del principio figuranti nella proposta della Commissione. L'ambito di applicazione è ulteriormente definito all'articolo 2, che al paragrafo 1 limita l'applicazione del principio di disponibilità alla fase precedente l'avvio di un procedimento giudiziario, mentre prevede, ai paragrafi 2, 3 e 4, altre restrizioni più specifiche.

22. Al fine di comprendere le conseguenze della proposta è necessaria un'analisi più approfondita dei tre elementi essenziali summenzionati. I primi due elementi dell'ambito di applicazione sono di per sé ragionevolmente chiari. La definizione di «informazioni esistenti» è spiegata all'articolo 2, paragrafo 2, il quale precisa che la decisione quadro non comporta alcun obbligo di raccogliere e conservare le informazioni al solo scopo di renderle disponibili, mentre l'elenco di cui all'allegato II non può essere interpretato diversamente. È il terzo elemento essenziale, considerato sia singolarmente che in combinazione con i primi due elementi, a necessitare di ulteriori chiarimenti.

23. La proposta non precisa se per «informazioni disponibili» si intendono puramente le informazioni già controllate dalle autorità competenti o anche informazioni che possono essere potenzialmente ottenute da tali autorità. Secondo il GEPD, la proposta potrebbe tuttavia essere interpretata come riguardante entrambi i tipi di informazioni.

24. Infatti, mentre l'articolo 2, paragrafo 2, sembra suggerire un campo di applicazione più ristretto, specificando che la decisione quadro «non comporta alcun obbligo di raccogliere e registrare le informazioni […] al solo scopo di renderle disponibili», l'articolo 3, lettera a) consente un'interpretazione più ampia, affermando che per «informazioni» si intendono «le informazioni esistenti, elencate nell'allegato II».

25. L'allegato II menziona almeno due categorie di dati che sono generalmente controllati da autorità diverse da quelle di polizia. La prima categoria è quella delle informazioni relative all'immatricolazione dei veicoli. In molti Stati membri le banche dati contenenti tali informazioni non sono controllate dalle autorità incaricate dell'applicazione della legge, anche se sono da queste regolarmente consultate. È opportuno includere tali informazioni nell'ambito delle «informazioni disponibili» che, ai sensi dell'articolo 1, sono fornite alle autorità competenti omologhe degli altri Stati membri? La seconda categoria di dati figuranti nell'allegato II da menzionare è quella dei numeri di telefono e altri dati relativi alle comunicazioni: è opportuno considerare tali dati come «disponibili» anche quando non sono controllati da autorità competenti, bensì da società private?

26. Altre disposizioni della proposta, ed in particolare l'articolo 3, lettera d) e l'articolo 4, paragrafo 1, lettera c) corroborano inoltre la posizione secondo cui le «autorità designate» o perfino le «parti designate» possono controllare informazioni che sono «disponibili» per le «autorità competenti». Dal testo della proposta si desume inoltre che un'«autorità competente» di uno Stato membro è una delle autorità contemplate dall'articolo 29, primo trattino, del trattato UE, mentre qualsiasi autorità nazionale può essere considerata un'«autorità designata».

27. A parere del GEPD, l'applicazione del principio di disponibilità ad informazioni che sono controllate da autorità e parti designate porta a porsi i seguenti interrogativi:

— L'articolo 30, paragrafo 1, lettera b) del trattato UE costituisce una base giuridica sufficiente, considerato che le informazioni devono essere rese disponibili da autorità e parti designate ed essere estratte da banche dati che non rientrano nel quadro del terzo pilastro?

— La decisione quadro sulla protezione dei dati personali sarà d'applicazione, come si presume, ad esempio, all'articolo 8 della proposta?

— In caso negativo, il trattamento è conforme agli obblighi di cui alla direttiva 95/46/CE?

28. L'attuazione di un principio vasto come il «principio di disponibilità» necessita di una definizione chiara e precisa dei dati da considerare come disponibili. Il GEPD raccomanda pertanto di:

— chiarire l'ambito di applicazione;

— quale prima opzione, limitare l'ambito di applicazione del principio di disponibilità alle informazioni controllate dalle autorità competenti;

— quale seconda opzione, nel caso di un ambito di applicazione più ampio, prevedere garanzie sufficienti per la protezione dei dati personali. Vanno presi in considerazione gli interrogativi formulati al punto 27.

**Altre questioni relative al campo di applicazione**

29. Ai sensi dell'articolo 2, paragrafo 1 della proposta, la decisione quadro si applica al trattamento delle informazioni prima dell'avvio di un procedimento giudiziario. Il suo campo di applicazione è più limitato rispetto a quello dalla proposta di decisione quadro sulla protezione dei dati personali, che si applica pienamente alla cooperazione giudiziaria in materia penale.

30. Tuttavia, secondo il GEPD tale limitazione non restringe di per sé il campo di applicazione della proposta alla sola cooperazione di polizia. Essa potrebbe anche includere la cooperazione giudiziaria in materia penale, poiché in alcuni Stati membri le autorità giudiziarie hanno competenza anche in materia di indagini penali, prima dell'avvio di un procedimento giudiziario. Il fatto che la proposta si fondi esclusivamente sull'articolo 30, paragrafo 1, lettera b) del trattato UE sembra tuttavia indicare che essa si applica unicamente alla cooperazione di polizia. Sarebbe opportuno chiarire tale aspetto.

31. L'attuale proposta si applica alla comunicazione di informazioni all'Europol mentre la proposta di decisione quadro sulla protezione dei dati personali esclude il trattamento dei dati personali da parte dell'Europol. Il GEPD consiglia di limitare lo scambio di informazioni con l'Europol all'ambito di competenza dell'Europol stesso, quale indicato nell'articolo 2 della convenzione Europol e nel relativo allegato. Si dovrebbe inoltre tener conto delle norme particolareggiate per lo scambio di dati con l'Europol, che sono state già stabilite in vari atti del Consiglio.

**Nessuna nuova banca dati contenente dati personali**

32. Il punto di partenza della proposta è che essa non condurrà alla creazione di nuove banche dati contenenti dati personali. In tal senso, l'articolo 2, paragrafo 2 è chiaro: la decisione quadro non comporta alcun obbligo di raccogliere e conservare le informazioni al solo scopo di renderle disponibili. Dal punto di vista della protezione dei dati questo è un elemento importante e positivo della proposta. Il GEPD rammenta il suo parere sulla proposta di direttiva relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici [1], nel quale sottolineava che gli obblighi giuridici che conducono alla creazione di consistenti basi di dati comportano particolari rischi per la persona cui si riferiscono i dati, tra cui quelli derivanti da un uso illecito dei medesimi.

33. Tuttavia:

— è importante fare in modo che la proposta non promuova un'interconnessione incondizionata delle banche dati e quindi una rete di banche dati che sarebbe difficile da controllare;

— esiste un'eccezione al punto di partenza summenzionato, ossia l'articolo 10 della proposta, che assicura la disponibilità on-line dei dati di indice. I dati di indice possono contenere dati personali o in ogni caso rivelarne l'esistenza.

**Accesso diretto e accesso indiretto alle informazioni**

34. La proposta contempla sia l'accesso alle informazioni diretto che quello indiretto. L'articolo 9 della proposta prevede l'accesso diretto on line alle informazioni contenute nelle banche dati a cui le autorità nazionali omologhe hanno accesso diretto on line. L'articolo 10 contempla l'accesso indiretto. I dati di indice delle informazioni non accessibili on line possono essere consultati on line dalle autorità competenti omologhe degli altri Stati membri e dall'Europol. Quando la consultazione dei dati di indice permette di individuare una corrispondenza, l'autorità in questione può compilare una domanda di informazioni e inviarla all'autorità designata per ottenere le informazioni identificate dai dati di indice.

35. L'accesso diretto non conduce alla creazione di nuove banche dati, ma necessita l'interoperabilità delle banche dati dei pertinenti sistemi equivalenti negli Stati membri. Inoltre, introdurrà necessariamente un nuovo utilizzo di banche dati già esistenti fornendo a tutte le autorità competenti degli Stati membri una struttura che sino ad ora era disponibile soltanto per le competenti autorità nazionali. L'accesso diretto comporterà automaticamente l'accesso alle banche dati da parte di un maggior numero di persone, con il conseguente aumento dei rischi di uso illecito.

[1] Parere del 26 settembre 2005 sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici e recante modifica della direttiva 2002/58/CE (COM (2005) 438 defin.).

36. In caso di accesso diretto da parte di un'autorità competente di un altro Stato membro, le autorità designate dello Stato membro d'origine non hanno alcun controllo sull'accesso e sul successivo utilizzo dei dati. Questa conseguenza dell'accesso diretto quale previsto dalla proposta deve essere adeguatamente presa in considerazione, dal momento che:

— sembra inficiare la facoltà, che hanno le autorità designate, di rifiutarsi di fornire le informazioni (a norma dell'articolo 14);

— dà adito a interrogativi circa la responsabilità dell'accuratezza e dell'aggiornamento dei dati, una volta dato l'accesso agli stessi. In che modo l'autorità designata dello Stato membro d'origine può assicurare che i dati siano tenuti aggiornati?

— Non è solo l'autorità designata a non essere più in grado di osservare tutti gli obblighi che le incombono in virtù della normativa sulla protezione dei dati; del pari, l'autorità nazionale dello Stato membro d'origine preposta alla protezione dei dati non può più verificare il rispetto di tali obblighi, dal momento che non ha alcuna competenza nei confronti delle autorità incaricate dell'applicazione della legge degli altri Stati membri.

— Questi problemi si pongono in misura ancora maggiore in caso di accesso alle banche dati da parte di autorità e parti designate diverse dalle autorità incaricate dell'applicazione della legge (vedansi i punti 25-28 del presente parere).

Questa conseguenza dell'accesso diretto è un motivo importante per subordinare l'adozione della presente proposta all'adozione di una decisione quadro sulla protezione dei dati personali. Resta da risolvere un problema: non è facile capire come le autorità designate possano rifiutarsi di fornire informazioni a norma dell'articolo 14.

37. Per quanto riguarda l'accesso indiretto attraverso dati di indice che forniscono informazioni su un sistema «hit/no hit»: non si tratta di un fenomeno nuovo. Su di essa si basa il funzionamento dei sistemi europei d'informazione su vasta scala, quali il Sistema d'Informazione Schengen. La creazione di un sistema di dati di indice ha il vantaggio di consentire agli Stati membri d'origine di controllare lo scambio di informazioni desunte dai loro archivi di polizia. Se la consultazione di dati di indice permette di individuare una corrispondenza, l'autorità richiedente può compilare una domanda di informazioni relativa alla persona cui si riferiscono i dati. Tale domanda può essere opportunamente valutata dall'autorità richiesta.

38. Tuttavia, è necessario procedere ad un'analisi adeguata, dato che la creazione di un sistema di dati di indice — in settori in cui questi sistemi a parte i sistemi europei di informazione su vasta scala, ancora non esistono — può creare nuovi rischi per le persone cui si riferiscono i dati. Il GEPD rileva che, sebbene i dati di indice non contengano molte informazioni sulle persone cui si riferiscono i dati, la loro consultazione può dare risultati altamente sensibili. Ne può emergere che una persona è schedata in un archivio di polizia per aver commesso dei reati.

39. È quindi della massima importanza che il legislatore europeo preveda norme adeguate, almeno per quanto riguarda la creazione dei dati di indice, la gestione dei sistemi di archiviazione dei medesimi e l'adeguata organizzazione dell'accesso a tali dati. A parere del GEPD, la proposta non è soddisfacente su questi punti. In questa fase, il GEPD formula tre osservazioni:

— La definizione dei dati di indice pecca di chiarezza. Non è chiaro se i dati di indice siano considerati metadati, chiavi primarie o entrambe le cose. La nozione di dati di indice va precisata, dal momento che incide direttamente sul livello di protezione dei dati e sulle garanzie necessarie.

— La proposta dovrebbe precisare il ruolo dei punti di contatto nazionali con riguardo ai dati di indice. Potrebbe essere necessario coinvolgere i punti di contatto nazionali, specialmente nei casi in cui l'interpretazione dei dati di indice richiede una conoscenza specialistica, ad esempio in caso di eventuale corrispondenza delle impronte digitali.

— La proposta demanda l'adozione delle norme necessarie per la creazione di dati di indice alla legislazione di attuazione, conformemente alla procedura di comitatologia di cui all'articolo 19. Sebbene possano rivelarsi necessarie disposizioni di attuazione, le norme fondamentali per la creazione dei dati di indice dovrebbero essere inserite nella decisione quadro stessa.

**Autorizzazione preventiva delle autorità giudiziarie**

40. Lo scambio di informazioni non impedisce agli Stati membri in cui è richiesta l'autorizzazione preventiva delle autorità giudiziarie di trasmettere le informazioni all'autorità richiedente quando dette informazioni sono assoggettate a controllo giudiziario nel paese richiesto. Ciò è importante dal momento che, da un'indagine sulla competenza della polizia a scambiare dati personali [1] è emerso che non in tutti gli Stati membri la polizia può accedere autonomamente a tali dati. Secondo il GEPD, il principio di disponibilità dovrebbe lasciare impregiudicato l'obbligo previsto dal diritto nazionale di ottenere un'autorizzazione preventiva per le informazioni, o dovrebbe quanto meno definire regole specifiche riguardanti le categorie di dati per le quali deve essere ottenuta un'autorizzazione preventiva, che saranno applicabili in tutti gli Stati membri.

[1] Risposte ad un questionario sulla decisione quadro relativa alla semplificazione dello scambio di informazioni ed intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge, in particolare con riguardo ai reati gravi, compresi gli atti terroristici (Doc. del Consiglio n.5815/1/05).

41. Tale obbligo andrebbe interpretato in collegamento con l'articolo 11, paragrafo 2 della proposta di decisione quadro sulla protezione dei dati personali, il quale prevede anch'esso che lo Stato membro che trasmette i dati abbia voce in capitolo in merito all'utilizzo dei dati nello Stato membro a cui questi sono stati trasmessi. Il GEPD sottolinea l'importanza di questo principio, necessario per assicurare che la disponibilità non porti all'elusione di una legislazione nazionale restrittiva sull'ulteriore utilizzo dei dati personali.

### Osservazione finale

42. Questi elementi richiedono elevati standard di protezione dei dati. Si dovrebbe provvedere specialmente ad assicurare il principio della limitazione delle finalità e dell'ulteriore trattamento nonché l'accuratezza e l'affidabilità delle informazioni cui viene dato accesso (cfr. il parere del GEPD sulla proposta di decisione quadro sulla protezione dei dati personali, punti IV.2 e IV.6).

## V. ALTRI APPROCCI

### Proposta della Svezia

43. La proposta della Svezia non è limitata a particolari tipi di informazioni, bensì abbraccia tutte le informazioni *e l'intelligence*, comprese le informazioni e l'intelligence custodite da autorità diverse da quelle preposte all'applicazione della legge. La proposta promuove la cooperazione fissando dei tempi di risposta alle domande di informazioni e sopprimendo la discriminazione tra gli scambi di informazioni all'interno di uno Stato membro e quelli transfrontalieri. Non prevede misure supplementari atte ad assicurare che l'accesso alle informazioni sia effettivo. È quindi comprensibile che la Commissione non consideri di per sé soddisfacente, in quanto strumento in materia di disponibilità ([1]) adeguato, la proposta svedese.

44. Dal punto di vista della protezione dei dati, l'approccio della proposta della Svezia ha le seguenti implicazioni generali:

— Il fatto che la proposta sia strettamente limitata al trattamento dei dati esistenti e non porti alla creazione di nuove banche dati, né tantomeno alla creazione di «dati di indice», è positivo.

— Tuttavia, l'assenza di «dati di indice» non è, per definizione, un elemento positivo. I dati di indice, se opportunamente protetti, possono facilitare una ricerca mirata e quindi meno intrusiva, di dati aventi carattere sensibile. Possono inoltre permettere di filtrare meglio le domande e consentire una più accurata sorveglianza.

— La proposta porta comunque ad un aumento dello scambio transfrontaliero di dati personali, con rischi in termini di protezione di tali dati, anche perché viene intaccata la competenza degli Stati membri a controllare pienamente i soggetti che si scambiano dati. Essa non dovrebbe essere adottata indipendemente dall'adozione della decisione quadro sulla protezione dei dati personali.

([1]) Cfr. Documento di lavoro della Commissione allegato alla proposta di decisione quadro del Consiglio sullo scambio di informazioni in virtù del principio di disponibilità, SEC 2005 (1207) del 12.10.2005.

### Trattato di Prüm

45. Il trattato di Prüm ha un approccio diverso all'attuazione del principio di disponibilità. Mentre la presente proposta di decisione quadro ha un approccio generale — che non prevede norme specifiche per lo scambio di particolari tipi di informazioni, bensì è applicabile a tutti i tipi di informazioni, a condizione che figurino nell'elenco dell'allegato II (cfr. punti 21-28 del presente parere) —, l'approccio del trattato di Prüm è graduale.

46. Tale approccio è talvolta denominato «approccio per singoli campi di dati» («data field-by-data field approach»). Si applica a particolari tipi di informazioni (DNA, dati relativi alle impronte digitali e all'immatricolazione dei veicoli) e prevede l'obbligo di tenere conto della particolare natura dei dati. Il trattato stabilisce l'obbligo di creare e mantenere schedari di analisi del DNA per l'investigazione dei reati. Un obbligo analogo vige per i dati relativi alle impronte digitali. Per quanto riguarda i dati relativi all'immatricolazione dei veicoli, l'accesso diretto va accordato ai punti di contatto nazionali degli altri Stati membri.

47. L'approccio del trattato di Prüm dà luogo a tre tipi di osservazioni.

48. In primo luogo, è ovvio che il GEPD non avalla il processo che ha portato alla firma di questo trattato, al di fuori del quadro istituzionale dell'Unione europea e quindi senza un reale coinvolgimento della Commissione. Inoltre, ne consegue che non vi è alcun controllo democratico da parte del Parlamento europeo né un controllo giurisdizionale da parte della Corte di giustizia e vi sono quindi minori garanzie che tutti gli interessi (pubblici) siano ugualmente presi in considerazione, compreso l'obiettivo della protezione dei dati. In altri termini, le istituzioni dell'Unione europea non hanno l'opportunità di valutare — prima che il sistema sia instaurato — l'impatto delle scelte operate in materia di politica di protezione dei dati personali.

49. In secondo luogo, è evidente che alcuni elementi del trattato di Prüm sono decisamente più intrusivi per le persone cui si riferiscono i dati rispetto a quanto prevede la proposta di decisione quadro sulla disponibilità. Il trattato conduce necessariamente alla creazione di nuove banche dati che di per sé presentano dei rischi per la protezione dei dati personali. La necessità e la proporzionalità della creazione di queste nuove banche dati andrebbero comprovate e dovrebbero essere previste adeguate garanzie per la protezione dei dati personali.

**Un approccio per singoli campi di dati («data field-by-data field approach»)**

50. In terzo luogo, come detto in precedenza, il trattato adotta un approccio per singoli campi di dati («data field-by-data field approach»). Il GEPD ha già menzionato nel presente documento, le difficoltà e le incertezze connesse al contesto in cui deve essere attuato il principio di disponibilità. Pertanto, a giudizio del GEPD, è preferibile non instaurare un sistema per un'intera gamma di dati ma iniziare piuttosto con un approccio più cauto, applicato a un solo tipo di dati e valutare in che misura il principio di disponibilità possa costituire un efficace ausilio all'applicazione della legge e quali siano i rischi specifici in relazione alla protezione dei dati personali. Sulla base di questa esperienza, il sistema potrebbe essere esteso eventualmente ad altri tipi di dati e/o essere modificato, al fine di renderlo più efficace.

51. L'approccio per singoli campi di dati risponderebbe inoltre meglio al principio di proporzionalità. Secondo il GEPD, la necessità di migliorare gli scambi transfrontalieri di dati ai fini dell'applicazione della legge potrebbe giustificare l'adozione di uno strumento giuridico a livello di Unione, ma per essere proporzionato lo strumento dovrebbe essere atto a conseguire il suo obiettivo, che potrà essere definito in modo più appropriato dopo un periodo di esperienza pratica. Inoltre, lo strumento non dovrebbe nuocere in misura sproporzionata alle persone cui si riferiscono i dati. Lo scambio dovrebbe limitarsi unicamente ai tipi di dati strettamente necessari, ed eventualmente essere anonimo ed essere effettuato nel rispetto di rigorosi requisiti in materia di protezione dei dati.

52. Inoltre, un approccio più cauto, quale quello auspicato dal GEPD — eventualmente in aggiunta all'approccio per singoli campi di dati — potrebbe consistere anche nell'iniziare l'attuazione del principio di disponibilità solo con l'accesso indiretto, attraverso i dati di indice. Il GEPD ritiene che questo punto meriti un esame in una fase successiva dell'iter legislativo.

## VI. **QUALI DATI?**

53. L'allegato II elenca i tipi di informazioni che possono essere ottenute in base alla decisione quadro proposta. Tutti e sei i tipi di informazioni ivi elencati sono dati personali nella maggior parte dei casi in quanto comportano tutti un collegamento con una persona identificata o identificabile.

54. Ai sensi dell'articolo 3, lettera g) della proposta, per dati di indice s'intendono «i dati che servono a identificare chiaramente le informazioni e che possono essere consultati mediante una routine di ricerca per accertare se le informazioni siano disponibili o meno». Nell'«Approccio per l'attuazione del principio di disponibilità» [1] sono definiti dati di indice i seguenti dati:

— i dati identificativi delle persone interessate;

— un numero d'identificazione degli oggetti interessati (veicoli, documenti);

— impronte digitali/foto digitali.

Un altro tipo di dati che potrebbero rientrare nella suddetta definizione sono i profili di DNA. Questo elenco evidenzia che i dati di indice possono contenere dati personali, e che è pertanto necessaria una protezione adeguata.

55. Il GEPD affronta specificamente la questione dei profili di DNA. L'analisi del DNA si è dimostrata di grande utilità nelle indagini penali, e un efficace scambio di dati sul DNA può essere essenziale per lottare contro la criminalità. Tuttavia, è indispensabile definire chiaramente il concetto di dati sul DNA e tener conto adeguatamente delle caratteristiche specifiche di tali dati. In effetti, dal punto di vista della protezione dei dati vi è una notevole differenza tra i campioni di DNA e i profili di DNA.

56. I campioni di DNA (spesso prelevati e conservati dalle autorità incaricate dell'applicazione della legge) dovrebbero essere considerati particolarmente sensibili, in quanto possono più facilmente contenere l'intero «quadro» del DNA. Possono fornire informazioni sulle caratteristice genetiche e sullo stato di salute di una persona, il che può servire per motivi completamente diversi, come dare pareri medici a singole persone o a giovani coppie.

57. Al contrario, i profili di DNA contengono soltanto alcune informazioni parziali sul DNA, estratte dal campione di DNA: esse possono essere utilizzate per verificare l'identità di una persona, ma in linea di massima non ne rivelano le caratteristiche genetiche. Tuttavia, i progressi scientifici possono accrescere il numero di informazioni ricavabili dai profili di DNA: quel che in un dato momento è considerato un profilo di DNA «innocuo», potrebbe rivelare successivamente molte più informazioni di quanto non sia prevedibile e necessario, in particolare informazioni riguardanti le caratteristiche genetiche di una persona. Le informazioni che possono essere ottenute dai profili di DNA andrebbero pertanto considerate come dinamiche.

58. In questa prospettiva, il GEPD rileva che sia il trattato di Prüm sia la proposta della Commissione promuovono lo scambio di dati sul DNA tra autorità incaricate dell'applicazione della legge, ma lo fanno in modo sostanzialmente diverso.

[1] Documento della presidenza al Consiglio del 5 aprile 2005 (doc. n.: 7641/05).

59. Il GEPD si rallegra che proposta della Commissione non imponga l'obbligo di raccogliere dati sul DNA e limiti chiaramente lo scambio di questi ultimi ai profili di DNA. L'allegato II definisce i profili di DNA attraverso un elenco comune iniziale di marcatori del DNA utilizzati per l'analisi forense del DNA negli Stati membri. Tale elenco, basato sui sette marcatori del DNA della serie europea standard (European Standard Set — ESS) definiti nell'allegato I della risoluzione del Consiglio del 25 giugno 2001 sullo scambio dei risultati delle analisi del DNA ([1]), garantisce che i profili di DNA non contengano, al momento in cui sono estratti, informazioni su specifiche caratteristiche ereditarie.

60. Il GEPD sottolinea che la suddetta risoluzione del Consiglio contiene alcune garanzie estremamente importanti, specificamente connesse alla natura dinamica dei profili di DNA. La parte III della risoluzione, dopo aver limitato gli scambi dei risultati dell'analisi del DNA alle «zone cromosomiche […], che notoriamente non forniscono informazioni su specifiche caratteristiche ereditarie», raccomanda infatti agli Stati membri di non impiegare più i marcatori del DNA che, a seguito di sviluppi scientifici, permettano di fornire informazioni su specifiche caratteristiche ereditarie.

61. Il trattato di Prüm adotta un approccio diverso, in quanto obbliga le parti contraenti a creare e mantenere archivi di analisi del DNA per l'investigazione dei reati. Comporta pertanto la creazione di nuove banche dati del DNA e un potenziamento della raccolta di dati sul DNA. Inoltre, non chiarisce quale tipo di dati siano inseriti negli «archivi di analisi del DNA» e non tiene conto dell'evoluzione dinamica dei profili di DNA.

62. Il GEPD sottolinea che qualsiasi strumento giuridico che preveda scambi di dati sul DNA dovrebbe:

— limitare e definire chiaramente il tipo di informazioni sul DNA che possono essere scambiate (anche in relazione alla differenza fondamentale tra campioni di DNA e profili di DNA);

— stabilire norme tecniche comuni per evitare che l'utilizzo di prassi diverse in materia di banche dati forensi del DNA negli Stati membri possa creare difficoltà e falsare i risultati al momento dello scambio dei dati;

— prevedere adeguate garanzie giuridicamente vincolanti per evitare che gli sviluppi scientifici permettano di ottenere dai profili di DNA dati personali non solo sensibili, ma anche non necessari ai fini per i quali sono stati raccolti.

([1]) GU C 187, pag. 1.

63. In questa prospettiva il GEPD conferma e completa in questa sede le osservazioni già formulate nel suo parere relativo alla decisione quadro sulla protezione dei dati personali (punto 80). In tale parere il GEPD sottolineava, con riguardo ai dati sul DNA, la necessità di prevedere garanzie specifiche, in modo da assicurare: che le informazioni disponibili possano essere utilizzate soltanto per l'identificazione di persone ai fini della prevenzione, dell'individuazione e dell'investigazione dei reati; che il livello di accuratezza dei profili di DNA sia adeguatamente preso in considerazione e possa essere contestato dalla persona interessata mediante strumenti prontamente disponibili; che sia pienamente garantito il rispetto della dignità delle persone ([2]).

64. Queste considerazioni portano inoltre alla conclusione che la normativa sulla creazione di archivi del DNA e sullo scambio di dati provenienti da tali archivi dovrebbe essere adottata soltanto previa realizzazione di una valutazione dell'impatto, in cui si siano potuti considerare adeguatamente vantaggi e rischi. Il GEPD raccomanda che nella normativa stessa sia previsto l'obbligo di valutazione periodica dopo la sua entrata in vigore.

65. Infine, nell'allegato II sono elencati gli altri tipi di informazioni che possono essere scambiate, tra cui figurano informazioni provenienti da soggetti privati, in quanto i numeri di telefono e gli altri dati relativi alle comunicazioni, nonché i dati sul traffico, provengono solitamente da operatori telefonici. Nella relazione si conferma che gli Stati membri sono tenuti a fare in modo che le informazioni utili per le attività di contrasto controllate dalle autorità o da soggetti privati designati a tal fine, siano condivise con le autorità competenti omologhe degli altri Stati membri e con l'Europol. Considerato che la proposta contempla i dati personali provenienti da soggetti privati, il quadro giuridico applicabile dovrebbe, secondo il GEPD, contenere garanzie supplementari per proteggere le persone cui si riferiscono i dati, in particolare quanto all'accuratezza dei dati stessi.

## VII. **PRINCIPI IN MATERIA DI PROTEZIONE DEI DATI**

66. La proposta di decisione quadro del Consiglio non contiene, al contrario di altri strumenti, come il trattato di Prüm o la proposta svedese, norme specifiche in materia di protezione dei dati personali. La mancanza di precise disposizioni al riguardo nella proposta sulla disponibilità è accettabile solo nella misura in cui le norme generali contenute nella proposta di decisione quadro sulla protezione dei dati nell'ambito del terzo pilastro siano pienamente applicabili e garantiscano una protezione sufficiente. Inoltre, le norme sulla protezione dei dati personali stabilite da strumenti specifici, come la proposta svedese e il trattato di Prüm, non dovrebbero abbassare il livello di protezione assicurato dal quadro generale. Il GEPD raccomanda di aggiungere una clausola specifica sugli eventuali conflitti tra le varie norme in materia di protezione dei dati.

([2]) In tale contesto cfr. anche la relazione del Consiglio d'Europa, del febbraio 2005, sull'applicazione dei principi della convenzione 108 alla raccolta e al trattamento dei dati biometrici personali (Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of personal biometric data).

67. In questa fase, il GEPD desidera nuovamente sottolineare, ricordando il parere da lui emesso con riguardo alla decisione quadro sulla protezione dei dati personali, l'importanza di disporre di norme sulla protezione dei dati che siano coerenti ed esaurienti in relazione alla cooperazione tra autorità di contrasto, e che valgano per tutti i trattamenti. Il GEPD ribadisce quindi gli altri punti contenuti nel suddetto parere. Nel presente punto sottolinea i seguenti elementi in materia di protezione dei dati:

— Trattamento legittimo dei dati personali. Il GEPD sostiene l'approccio secondo cui le informazioni possono essere rese disponibili solo a condizione di essere state raccolte in modo lecito (come indicato nell'articolo 2, paragrafo 2 per le informazioni raccolte mediante misure coercitive). Il trattamento legittimo dei dati personali assicurerebbe inoltre che le informazioni rese disponibili e scambiate possano essere utilizzate correttamente anche nell'ambito di un procedimento giudiziario. In effetti, sebbene le informazioni trattate dopo l'avvio di un procedimento non rientrino nel campo di applicazione dello strumento proposto, è comunque probabile che le informazioni scambiate precedentemente dalle autorità incaricate dell'applicazione della legge finiscano in procedimenti giudiziari.

— Qualità dei dati personali. Questo punto è di particolare importanza, in quanto, in virtù del principio di disponibilità, le informazioni saranno utilizzate da autorità incaricate dell'applicazione della legge operanti al di fuori del contesto in cui i dati sono stati raccolti. Tali autorità hanno addirittura l'accesso diretto alle banche dati di altri Stati membri. La qualità dei dati personali può essere garantita solo verificandone regolarmente e adeguatamente l'esattezza, distinguendo le informazioni in funzione delle varie categorie di persone interessate (vittime, sospettati, testimoni, ecc.) e, se necessario, indicando il livello di accuratezza (cfr. il parere del GEPD sulla protezione dei dati personali, punto IV.6).

Questi elementi evidenziano ancora una volta perché le norme in materia di protezione dei dati personali, in particolare quelle relative all'accuratezza, debbano applicarsi a tutti i tipi di trattamento, anche quelli effettuati a livello nazionale. Altrimenti, i dati personali ai quali è possibile accedere direttamente potrebbero essere scorretti o non aggiornati, a scapito dei diritti di coloro cui si riferiscono e dell'efficienza delle indagini.

— Limitazione delle finalità. Conformemente al principio di disponibilità, i dati personali sono accessibili alle autorità competenti omologhe degli altri Stati membri. Tuttavia, le competenze delle autorità incaricate dell'applicazione della legge possono variare considerevolmente da un paese all'altro. È pertanto essenziale provvedere affinché il principio fondamentale della limitazione delle finalità sia rispettato nonostante i diversi ambiti di competenza delle autorità competenti che procedono allo scambio di dati. Le informazioni raccolte e trattate da una determinata autorità per una certa finalità non possono quindi essere utilizzate per una finalità diversa solo in virtù delle differenti (eventualmente più ampie) competenze dell'autorità che li riceve.

Pertanto, il GEPD si compiace dell'articolo 7 della proposta di decisione quadro, che va visto come una precisazione delle norme generali contenute nella proposta di decisione quadro sulla protezione dei dati personali. Inoltre, il GEPD rileva che la valutazione dell'equivalenza tra le varie autorità (che nella proposta in esame ha luogo secondo la procedura di comitatologia) dovrebbe essere effettuata con attenzione e nel debito rispetto del principio di limitazione delle finalità.

— Termini per la conservazione delle informazioni scambiate. Anche questo elemento va considerato alla luce del principio di limitazione delle finalità: le informazioni ottenute o scambiate per una finalità dovrebbero essere cancellate non appena non più necessarie per quella finalità. Ciò permetterebbe di evitare inutili doppioni nelle banche dati, fermo restando che le autorità competenti sarebbero autorizzate ad accedere nuovamente alle informazioni disponibili (aggiornate) qualora ciò si rivelasse necessario per un'altra finalità legittima.

— Registrazione delle informazioni trasmesse conformemente al principio di disponibilità. La registrazione dovrebbe essere effettuata da entrambe le parti: sia nello Stato membro richiesto che in quello richiedente. Sarebbe opportuno tenere parimenti registri relativi all'accesso e non solo registri relativi allo scambio di informazioni (cfr. il parere sulla protezione dei dati personali, punto 133), anche allo scopo di far sì che le autorità nazionali competenti possano avere fiducia reciproca e non perdano completamente il controllo delle informazioni disponibili. L'esigenza di tracciabilità implica anche la possibilità di aggiornare e/o correggere le informazioni.

— Diritti delle persone cui si riferiscono i dati. I sistemi per lo scambio di informazioni tra autorità incaricate dell'applicazione della legge accrescono il numero di situazioni in cui dati personali vengono (temporaneamente) trattati nel contempo da autorità competenti di Stati membri diversi. Ne consegue, da un lato, che sarebbe opportuno stabilire norme comuni a livello dell'UE sui diritti delle persone cui si riferiscono i dati e, dall'altro, che queste ultime dovrebbero poter esercitare i loro diritti, nella misura consentita dalle norme sulla protezione dei dati nell'ambito del terzo pilastro, sia nei confronti delle autorità che rendono disponibili i dati che di quelle che vi accedono e li trattano.

— Sorveglianza. Il GEPD sottolinea che, a seconda dei casi, possono essere competenti a controllare il trattamento dei dati personali effettuato in base alla proposta in esame più autorità nazionali di sorveglianza. A tale riguardo, l'accesso diretto on-line alle informazioni in materia di applicazione della legge richiede un rafforzamento della sorveglianza e del coordinamento da parte delle autorità nazionali preposte alla protezione dei dati.

## VIII. **CONCLUSIONI**

### Conclusioni generali relative al principio di disponibilità

68. Il GEPD coglie l'occasione per presentare in questo parere alcuni elementi di base generali sul tema dello scambio di informazioni in materia di applicazione della legge e sugli approcci per disciplinare questo ambito. Il GEPD resta disponibile per una nuova consultazione in una fase successiva, quando saranno intervenuti sviluppi nell'iter legislativo della proposta in esame e di altre proposte correlate.

69. Secondo il GEPD, il principio di disponibilità dovrebbe essere attuato in uno strumento giuridico vincolante attraverso un approccio più cauto e graduale applicato a un solo tipo di dati, per valutare in che misura possa costituire un efficace ausilio all'applicazione della legge e quali siano i rischi specifici in relazione alla protezione dei dati personali. Questo approccio più cauto potrebbe consistere anche nell'iniziare l'attuazione del principio di disponibilità solo con l'accesso indiretto, attraverso i dati di indice. Sulla base di questa esperienza, il sistema potrebbe essere esteso eventualmente ad altri tipi di dati e/o essere modificato, al fine di renderlo più efficace.

70. Non dovrebbe essere adottato alcuno strumento giuridico di attuazione del principio di disponibilità senza che siano state precedentemente adottate garanzie essenziali in materia di protezione dei dati, quali quelle indicate nella proposta di decisione quadro sulla protezione dei dati personali.

### Raccomandazioni di modifica della proposta in esame

71. Il GEPD raccomanda di chiarire l'ambito di applicazione del principio di disponibilità nel modo seguente:

    — aggiungere una definizione chiara e precisa dei dati che saranno considerati disponibili;

    — quale prima opzione, limitare l'ambito di applicazione del principio di disponibilità alle informazioni controllate dalle autorità competenti;

    — quale seconda opzione, nel caso di un ambito di applicazione più ampio, prevedere garanzie sufficienti per la protezione dei dati personali. Vanno presi in considerazione gli interrogativi formulati al punto 27 del presente parere.

72. Il GEPD formula le seguenti osservazioni per quanto riguarda l'accesso diretto alle banche dati da parte di un'autorità competente di un altro Stato membro:

    — la questione deve essere affrontata adeguatamente in quanto, in caso di accesso diretto, le autorità designate dello Stato membro di origine non hanno alcun controllo sull'accesso ai dati e sul loro ulteriore utilizzo;

    — la proposta può non promuovere un'interconnessione incondizionata delle banche dati e quindi una rete di banche dati, che sarebbe difficile da controllare.

73. La decisione quadro dovrebbe essere più precisa quanto all'instaurazione di un sistema di dati di indice. In particolare:

    — la proposta dovrebbe prevedere norme adeguate, almeno per quanto riguarda la creazione di dati di indice, la gestione dei sistemi di archiviazione dei medesimi e l'adeguata organizzazione dell'accesso a tali dati;

    — andrebbe chiarita la definizione dei dati di indice;

    — la proposta dovrebbe precisare il ruolo dei punti di contatto nazionali con riguardo ai dati di indice;

    — le norme fondamentali per la creazione dei dati di indice dovrebbero essere inserite nella decisione quadro stessa e non demandate alla legislazione di attuazione conformemente alla procedura di comitatologia.

74. Il GEPD sottolinea che — nella misura in cui prevede scambi di dati sul DNA — la proposta dovrebbe:

    — limitare e definire chiaramente il tipo di informazioni sul DNA che possono essere scambiate (anche in relazione alla differenza fondamentale esistente tra campioni di DNA e profili di DNA);

    — stabilire norme tecniche comuni per evitare che l'utilizzo di prassi diverse in materia di banche dati forensi del DNA negli Stati membri possa creare difficoltà e falsare i risultati al momento dello scambio dei dati;

    — prevedere adeguate garanzie giuridicamente vincolanti per evitare che gli sviluppi scientifici permettano di ottenere dai profili di DNA dati personali non solo sensibili, ma anche inutili ai fini per i quali sono stati raccolti;

    — essere adottata soltanto previa realizzazione di una valutazione dell'impatto.

75. Il GEPD consiglia di limitare lo scambio di informazioni con l'Europol all'ambito di competenza dell'Europol stesso, quale indicato nell'articolo 2 della convenzione Europol e nel relativo allegato.

Bruxelles, 28 febbraio 2006

Peter HUSTINX

*Garante europeo della protezione dei dati*