ARTICOLO 29 - Gruppo per la tutela dei dati personali

1868/05/IT
WP 113

Parere 4/2005 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE (COM(2005)438 definitivo del 21.9.2005)

Adottato il 21 ottobre 2005

RELAZIONE

La proposta della Commissione europea di una direttiva sulla conservazione di dati ci pone di fronte a una decisione storica.

La conservazione dei dati relativi al traffico interferisce con il diritto inviolabile e fondamentale alla riservatezza delle comunicazioni.

Qualunque restrizione di questo diritto fondamentale deve essere motivata da necessità impellente, dovrebbe essere autorizzata solo in casi eccezionali e subordinata a garanzie adeguate.

I fornitori di servizi di comunicazioni accessibili al pubblico sarebbero tenuti, come mai in passato, a memorizzare miliardi di dati sulle comunicazioni di ogni singolo cittadino a fini investigativi.

Il terrorismo pone la nostra società di fronte a una sfida reale e stringente. I governi devono reagire in modo da rispondere effettivamente all'esigenza dei loro cittadini di vivere in pace e sicurezza senza intaccarne i diritti individuali - come il diritto alla riservatezza dei dati - che sono un elemento fondante delle nostre società democratiche.

L'iniziativa della Commissione europea potrebbe comportare in ultima analisi la definizione di periodi di conservazione più brevi di quelli contemplati in altre proposte recenti.

Il gruppo si chiede se la giustificazione di una conservazione obbligatoria e generale dei dati presentata dalle autorità competenti degli Stati membri si fondi su prove chiare e trasparenti. Il gruppo dubita inoltre della fondatezza dei periodi di conservazione proposti nel progetto di direttiva.

Come si è appena detto, occorre dimostrare chiaramente e addurre la prova che la conservazione obbligatoria e generale dei dati è giustificata. Lo stesso dicasi per i periodi massimi che sarebbero d'applicazione. In ogni caso, andrebbero anche indicate con chiarezza le condizioni in cui le autorità competenti potrebbero accedere ai dati e usarli nella lotta alla minaccia del terrorismo.

Le finalità della conservazione dei dati andrebbero enunciate chiaramente nella direttiva con riguardo alla lotta al terrorismo e alla criminalità organizzata, e non già a "reati gravi" non determinati.

Bisogna considerare che esistono approcci meno invasivi della vita privata, come la procedura *quick-freeze* (congelamento rapido).

Il periodo di conservazione dei dati dovrebbe, se del caso, essere quanto più breve e costituire il limite massimo applicabile a tutti gli Stati membri, i quali resterebbero comunque liberi di fissare periodi più brevi. Le misure eventualmente introdotte dovrebbero ricevere ampia pubblicità.

Le prove che giustificano tali misure dovrebbero essere oggetto di valutazione periodica. Sulla base di questa valutazione, da effettuarsi come minimo ogni due o tre anni e da rendere pubblica, è opportuno che le previste misure di conservazione dei dati siano limitate nel tempo secondo il concetto della "normativa a tempo determinato". Si ritiene adeguato un termine di tre anni.

In ogni caso è inaccettabile che nel quadro giuridico europeo esistente si impongano tali obblighi ai fornitori di servizi di comunicazione senza aver predisposto anzitutto garanzie adeguate e specifiche.

Per finire, il gruppo propone venti garanzie specifiche, riguardanti in particolare i requisiti applicabili ai beneficiari e al trattamento ulteriore dei dati, la necessità di autorizzazioni e controlli, le misure applicabili ai fornitori di servizi anche in termini di sicurezza e separazione logica dei dati, la definizione delle categorie dei dati interessati e il loro aggiornamento, e la necessità di escludere i dati relativi al contenuto.

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995,

visti gli articoli 29 e 30, paragrafi 1, lettera a), e 3 della richiamata direttiva e l'articolo 15, paragrafo 3, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 giugno 2002,

visto il suo regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il seguente parere:

I. Antefatti

Nell'ambito delle iniziative europee di lotta al terrorismo e alla criminalità organizzata, il 21 settembre scorso la Commissione europea ha presentato una "*proposta di direttiva riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE*[1]".

La questione riveste notevole importanza per tutti i cittadini.

La libertà e la riservatezza della corrispondenza e di tutte le altre forme di comunicazione sono pilastri delle moderne società democratiche. Svariati documenti, anche carte costituzionali, ne riconoscono l'inviolabilità, che è in particolare sancita dalla convenzione europea dei diritti dell'uomo sui cui è fondato il diritto comunitario.

La proposta di direttiva ci pone di fronte a una decisione storica. Suo obiettivo è introdurre, per la prima volta, l'obbligo su scala europea di conservare miliardi di dati sulle comunicazioni di ogni singolo cittadino a fini investigativi. A norma del diritto comunitario, attualmente questi dati non sono memorizzati, oppure sono conservati dai fornitori di comunicazioni elettroniche su base puramente temporanea, ed esclusivamente a fini contrattuali.

La conservazione dei dati relativi al traffico interferisce con il diritto fondamentale alla riservatezza delle comunicazioni, garantito all'individuo dall'articolo 8 della convenzione europea dei diritti dell'uomo. In una società democratica, l'eventuale ingerenza nell'esercizio di questo diritto fondamentale è giustificata se necessaria per la sicurezza nazionale, e può in ultima analisi risolversi nel controllo e rilevamento di tutti i contatti e le relazioni di un individuo, nonché dei luoghi in cui quelli si svolgono e dei mezzi usati a tal fine. La Corte europea dei diritti dell'uomo ha inoltre evidenziato il rischio intrinseco alla sorveglianza in segreto di minare o anche distruggere la democrazia nell'intento di difenderla; la Corte ha altresì affermato che gli Stati non possono adottare, in nome della lotta contro lo spionaggio e il terrorismo, una qualunque misura che giudichino appropriata[2].

[1] [COM (2005) 438 definitivo] del 21.9.2005, *non ancora pubblicato nella GU.*
[2] Klass e altri c. Germania, punto 49.

Perciò, qualunque restrizione di questo diritto fondamentale deve essere motivata da necessità impellente, dovrebbe essere autorizzata solo in casi eccezionali e subordinata a garanzie adeguate. La conservazione dei dati sul traffico, compresi quelli relativi all'ubicazione, per fini connessi alle attività di contrasto, dovrebbe rispondere a condizioni rigorose[3], in particolare deve essere autorizzata solo per periodi limitati e se costituisce una misura necessaria, opportuna e proporzionata all'interno di una società democratica.

I poteri attribuiti agli organi di contrasto per combattere il terrorismo devono essere certo efficaci ma non illimitati, e quelle autorità non possono abusarne. Occorre raggiungere un giusto equilibrio per non compromettere il tipo di società che vogliamo tutelare. Un equilibrio più che mai importante se l'obiettivo è obbligare i fornitori di servizi di comunicazione a immagazzinare dati di cui sono i primi a non avere necessità. Di questo passo, non è escluso che si finisca per ottenere un controllo senza precedenti, permanente e pervasivo di tutti i tipi di comunicazione e movimento della totalità dei cittadini nella vita quotidiana. La mole impressionante di informazioni che andremmo così a conservare sarebbe davvero utile a fini investigativi solo in un numero limitato di casi.

Occorre inoltre considerare l'impatto di un obbligo così radicale di conservazione dei dati su alcune comunicazioni che sollevano problemi delicati in relazione a certe categorie di segreto professionale e/o investigativo, o a certe attività di istituzioni particolari, specificamente protette dalla legge.

Per questo motivo, da alcuni anni ormai il parere del gruppo ex articolo 29 e della conferenza delle autorità europee per la protezione dei dati è fermo e chiaro. In diverse occasioni dal 1997 il gruppo[4] e la conferenza europea[5] hanno messo in discussione la necessità di misure generali di conservazione dei dati.

---

[3] Si veda in particolare l'articolo 15, paragrafo 1, della direttiva 2002/58/CE.

[4] Si vedano i seguenti documenti (tutti disponibili su *http://europa.eu.int/comm/internal_market/privacy*):

-**Parere 9/2004** Progetto di decisione quadro [..] (documento del Consiglio n. 8958/04 del 28 aprile 2004). Una sintesi delle seguenti dichiarazioni è allegata al presente parere.
-**Parere 1/2003** sulla memorizzazione ai fini della fatturazione dei dati relativi al traffico.
-**Parere 5/2002** sulla dichiarazione dei commissari europei per la protezione dei dati alla conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni.
-**Parere 10/2001** sulla necessità di un approccio equilibrato alla lotta contro il terrorismo.
-**Parere 4/2001** sul progetto di convenzione sulla cibercriminalità del Consiglio d'Europa.
-**Parere 7/2000** sulla proposta della Commissione europea di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2000 COM (2000) 385.
-**Raccomandazione 3/99** sulla conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari.
-**Raccomandazione 3/99** relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni;
-**Raccomandazione 3/97** sull'anonimato su Internet.

[5] Cfr. le dichiarazioni adottate a Stoccolma (aprile 2000) e Cardiff (aprile 2002).

II. VALUTAZIONE PRELIMINARE E CONDIZIONI GENERALI

1. La conservazione dei dati può essere uno strumento utile nelle mani degli investigatori, ciò nondimeno le condizioni di cui sopra devono ricorrere e giustificarsi chiaramente.

Anzitutto, l'obiettivo di una tale misura andrebbe formulato molto chiaramente. In secondo luogo, occorre dimostrare chiaramente e addurre la prova che la conservazione obbligatoria e generale dei dati è giustificata. Lo stesso dicasi per i periodi massimi che sarebbero d'applicazione. In terzo luogo, andrebbero indicate con chiarezza le condizioni in cui le autorità competenti potrebbero accedere ai dati e usarli nella lotta alla minaccia del terrorismo.

Le prove addotte andrebbero quanto meno valutate periodicamente e i risultati pubblicati, considerando anche che l'introduzione di mezzi di sorveglianza generale dei cittadini potrebbe indurre le organizzazioni criminali e terroristiche a sviluppare strategie per evitare di usare certi mezzi. Ne conseguirebbe la necessità di escogitare nuovi metodi di sorveglianza ancora più rigorosi, scatenando una spirale di potenziali violazioni dei diritti fondamentali dei cittadini che sarà difficile arrestare. Inoltre, in questo modo cambierebbe il carattere della società che cerchiamo di preservare.

Il gruppo riconosce che alcune condizioni sono mutate nelle nostre società in relazione alla minaccia terroristica, ed è consapevole di quanto, a volte, in certe indagini alcuni dati possano essere utili se usati legittimamente. Il gruppo riconosce altresì che l'iniziativa della Commissione europea potrebbe in definitiva comportare l'introduzione di periodi massimi di conservazione più brevi di quelli prospettati in passato e per i quali il gruppo ha espresso parere sfavorevole, da ultimo nel parere 9/2004 adottato il 9 novembre 2004, WP 99.

Ciò nondimeno, le circostanze che giustificano la conservazione dei dati, pur basandosi verosimilmente su domande provenienti dalle autorità competenti degli Stati membri, non sembrano fondarsi su prove chiari e trasparenti. Allo stesso modo, non sembrano ancora convincenti i termini di conservazione proposti.

Esistono altri mezzi utili da considerare a fini investigativi, con un impatto minore sui diritti fondamentali del cittadino, come la cosiddetta procedura *quick freeze* nella quale né i fornitori di comunicazione né i fornitori di servizi Internet sono tenuti a memorizzare i dati sul traffico. Per esempio, nei casi che lo giustifichino, gli organi di contrasto consultano le società e chiedono di memorizzare certi dati. Quegli organi dispongono quindi di alcune settimane per raccogliere le prove necessarie per ottenere un provvedimento giudiziario. Solo allora potranno accedere ai dati.

In ogni caso, è necessario che un periodo di conservazione generale sia regolamentato con chiarezza: dovrebbe essere il più breve possibile e coincidere al massimo con il periodo di conservazione fissato per le finalità iniziali per cui i fornitori di servizi di comunicazione avevano registrato quei dati.

2. L'armonizzazione delle legislazioni nazionali attualmente proposta dalla Commissione dovrebbe chiarire che l'introduzione di un periodo di conservazione obbligatorio a livello europeo è basata su una valutazione della proporzionalità su scala europea, che tiene conto

anche del carattere transnazionale della criminalità organizzata e dei requisiti massimi di sicurezza di tutti gli Stati membri.

Bisognerebbe poi precisare che il periodo di conservazione dei dati di cui alla direttiva è da considerarsi la soglia massima armonizzata applicabile a tutti gli Stati membri.

Pertanto, dovrà essere chiarito che gli Stati membri non avranno facoltà di disporre periodi più lunghi rispetto alla direttiva, ma saranno liberi di prevedere periodi più brevi. Occorrerà anche ricordare che i dati devono essere cancellati alla fine dei citati periodi. Con queste premesse, l'attuale formulazione dell'articolo 11 della proposta di direttiva non è soddisfacente.

Il gruppo ex articolo 29 si compiace dell'inclusione nella proposta di un articolo (l'articolo 12) relativo a una valutazione periodica, da effettuarsi almeno ogni due anni.

Tale valutazione dovrebbe riguardare anche la necessità dei dati relativi al traffico usati dalle autorità di contrasto in casi specifici e identificati, e associare le autorità garanti della protezione dei dati. Gli esiti delle valutazioni andrebbero inoltre pubblicati.

Bisognerebbe tuttavia precisare che la citata valutazione non deve svolgersi su un periodo indeterminato, visto che la proposta si basa sulla valutazione concreta delle ipotesi e dei prerequisiti cui si riferisce. È pertanto opportuno che le previste misure di conservazione dei dati siano limitate nel tempo secondo il concetto della "normativa a tempo determinato". Il gruppo ritiene adeguato un termine di tre anni. Scaduto quel termine, dovrebbe cessare l'efficacia dei provvedimenti nazionali di attuazione che ordinano la conservazione dei dati, ferma restando la possibilità di iniziare l'analisi necessaria per la preparazione di una nuova decisione con cui il Consiglio e il Parlamento europeo approvano la nuova direttiva anche prima della scadenza del termine triennale.

Quanto al principio di proporzionalità, il gruppo ex articolo 29 si compiace anche del fatto che l'insieme di dati da conservare in relazione all'uso di Internet sia circoscritto. Al riguardo, bisogna inoltre preferire un insieme massimo di dati a un elenco minimo. In generale, i dati da conservare andrebbero limitati a quelli raccolti dai fornitori a fini tecnici o per esigenze di fatturazione.

È essenziale determinare l'accesso ai dati e le finalità del loro uso per garantire che le misure generali di conservazione dei dati siano accompagnate da garanzie massime, e sottoporre tali misure a controllo.

3. Le garanzie previste nell'ambito del quadro giuridico esistente in materia di protezione dei dati nel primo pilastro (direttive 95/46/CE e 2002/58/CE) dovrebbero essere specificate ulteriormente, in funzione del particolare contesto della conservazione dei dati sul traffico ai fini dell'azione di contrasto. Sono in effetti indispensabili garanzie specifiche per evitare che sia compromessa nella sostanza la protezione offerta dalla direttiva 2002/58/CE, in relazione in particolare al diritto alla riservatezza dei servizi di comunicazioni elettroniche accessibili al pubblico.

Il gruppo sostiene per altro la necessità di introdurre garanzie adeguate per il trattamento dei dati in settori che attualmente non rientrano nel campo di applicazione di quelle direttive.

Per questo motivo il gruppo ritiene, fra l'altro, che la proposta di direttiva dovrebbe già contemplare queste garanzie, o essere comunque valutata e adottata contestualmente a altri strumenti giuridici adeguati. In particolare, il gruppo crede che la "decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale" dovrà essere oggetto di una valutazione profonda anche in questo contesto.

Da ultimo, visto l'impatto dell'iniziativa sui diritti e le libertà fondamentali dei cittadini interessati, il gruppo pensa che sarebbe opportuno dare ampia pubblicità alle misure eventualmente introdotte.

III. ALTRE GARANZIE SPECIFICHE

In aggiunta a quanto sopra, il gruppo ritiene che occorra quanto meno affrontare i seguenti aspetti:

1. FINALITÀ

I dati dovrebbero essere conservati soltanto ai fini specifici della lotta al terrorismo e alla criminalità organizzata, e non già in relazione a "reati gravi" non determinati. Tale finalità limitata dovrebbe figurare anche nel titolo della proposta di direttiva.

2. BENEFICIARI

La direttiva dovrebbe prevedere che i dati siano messi a disposizione soltanto delle autorità di contrasto specificamente designate, se necessario per la prevenzione, la ricerca, l'accertamento e il perseguimento del terrorismo. Sarebbe inoltre opportuno rendere pubblico l'elenco di tali autorità designate.

3. DATA MINING

La prevenzione del terrorismo non dovrebbe comportare operazioni di *data mining* su ampia scala basate sulle informazioni di cui alla direttiva, in relazione alle abitudini di trasporto e comunicazione di soggetti non sospettati dalle autorità di contrasto. Occorre limitare l'accesso ai dati necessari nell'ambito di un'indagine specifica.

4. ULTERIORE TRATTAMENTO

Andrebbe escluso o rigorosamente limitato in forza di garanzie specifiche qualunque trattamento ulteriore dei dati conservati, a opera delle autorità di contrasto nell'ambito di altri procedimenti connessi, così come andrebbe impedito l'accesso ai dati ad altri organi di governo. Non è permessa l'applicazione di norme relative al settore delle comunicazioni elettroniche introdotte da strumenti giuridici europei precedenti, che contrasti con questo principio.

5. REGISTRI DI ACCESSO

Ogni estrazione di dati dovrebbe figurare in un registro. I registri dovrebbero essere a disposizione soltanto dell'autorità e/o dell'organo di cui al punto 6 che ne fanno richiesta, e delle autorità garanti della protezione dei dati in caso di controllo, e devono essere eliminati un anno dopo la loro costituzione.

6. CONTROLLO GIUDIZIARIO INDIPENDENTE

L'accesso ai dati dovrebbe, in linea di principio, essere debitamente autorizzato, caso per caso, da un'autorità giudiziaria, fatti salvi i paesi in cui la legge autorizza una possibilità specifica di

accesso, ed essere soggetto a controllo indipendente. Se del caso, le autorizzazioni dovrebbero precisare i dati richiesti per gli specifici casi in questione.

7. DESTINATARI

La direttiva dovrebbe definire chiaramente i fornitori di servizi di comunicazioni accessibili al pubblico interessati dagli obblighi. Nel caso di Internet, è necessario introdurre limitazioni per i fornitori di accesso e la comunicazione interpersonale (e-mail, Voice over IP).

8. IDENTIFICAZIONE

È importante che la direttiva chiarisca anche che non sussiste obbligo di identificazione quando non è necessario identificarsi ai fini della fatturazione o per altri fini contrattuali.

9. FINI DI ORDINE PUBBLICO

I fornitori di servizi di comunicazioni elettroniche accessibili al pubblico o di una rete pubblica di comunicazione non dovrebbero essere autorizzati a trattare, a fini personali, i dati conservati esclusivamente per motivi di ordine pubblico.

10. SEPARAZIONE DEI SISTEMI

In particolare, i sistemi di memorizzazione dei dati a fini di ordine pubblico dovrebbero essere logicamente separati dai sistemi usati per fini commerciali dai fornitori, e protetti con misure di sicurezza più incisive (per esempio, il criptaggio) che ne impediscano l'accesso e l'uso non autorizzato.

11. MISURE DI SICUREZZA

Le misure comunitarie dovrebbero stabilire standard minimi per le misure di sicurezza tecniche e organizzative imposte ai fornitori, indicando i requisiti generali di sicurezza fissati dalla direttiva 2002/58/CE.

12. TERZI

Le misure comunitarie dovrebbero precisare che l'accesso di terzi ai dati conservati è illegale.

13. DEFINIZIONI

Il testo dovrebbe comprendere una definizione chiara delle categorie di dati e una limitazione dei dati relativi al traffico.

14. ELENCO DEI DATI E MECCANISMI DI REVISIONE

È necessario che la direttiva specifichi direttamente l'elenco dei dati personali da conservare, in modo da permettere una valutazione accurata dell'impatto sui diritti e sulle libertà fondamentali dei cittadini interessati, che tenga conto sia dei rischi per la loro sfera personale, sia degli aspetti diretti a garantire la precisione e l'aggiornamento dei dati conservati. Qualunque proposta volta a modificare l'elenco delle categorie di dati da conservare deve passare attraverso una rigorosa verifica della necessità. Considerato l'impatto di queste misure sui diritti e sulle libertà fondamentali, la revisione del citato elenco dovrebbe svolgersi soltanto previa approvazione del Parlamento europeo e associando le autorità garanti della protezione dei dati. Andrebbe inoltre contemplata la partecipazione di rappresentanti delle associazioni di consumatori e di utenti, di altri organi non governativi rilevanti e delle associazioni europee del settore delle comunicazioni elettroniche. Date le premesse non sembra opportuno procedere alla revisione del citato elenco esperendo soltanto la procedura di comitato proposta dalla direttiva.

15. ESCLUSIONE DEI DATI RELATIVI AL CONTENUTO

Poiché si intende escludere dal campo di applicazione della direttiva il contenuto delle comunicazioni, sarebbe opportuno introdurre garanzie specifiche che distinguano in modo netto e effettivo fra dati relativi ai contenuti e dati relativi al traffico, sia per Internet (per esempio, solo i dati del log-in/log-off, o altre informazioni come i log del mail server, del web cache e del flusso IP), sia per la telefonia (conferenze telefoniche, fax, messaggeria, voce).

16. TENTATIVI MANCATI DI COMUNICAZIONE

Non dovrebbero essere comprese le diverse categorie di dati sul traffico connessi a tentativi mancati di comunicazione, mancando una valutazione profonda della loro adeguatezza alla luce dei principi citati.

17. DATI RELATIVI ALL'UBICAZIONE

La memorizzazione dei dati relativi all'ubicazione non dovrebbe andare oltre il Cell ID all'inizio della comunicazione.

18. CONTROLLO EFFETTIVO

È opportuno che siano garantiti controlli effettivi dell'uso iniziale e di usi ulteriori compatibili (compresa la copia) da parte delle autorità giudiziarie nell'ambito e ai fini di un procedimento penale, e delle autorità garanti della protezione dei dati per la protezione dei dati indipendentemente dall'esistenza di un'azione giudiziaria.

19. PUBBLICITÀ

La direttiva dovrebbe contemplare l'obbligo di informare adeguatamente tutti i cittadini dei singoli trattamenti potenzialmente eseguibili in applicazione delle sue misure.

20. COSTI

Il gruppo ex articolo 29 constata che spetta agli Stati membri rimborsare i costi supplementari sostenuti dai fornitori di servizi di comunicazioni elettroniche accessibili al pubblico e di una rete pubblica di comunicazione. Il gruppo desidera evidenziare l'importanza di questo aspetto limitatamente alle caratteristiche che hanno attinenza diretta con la protezione dei dati. Le misure di conservazione dei dati dovrebbero comportare anche il rimborso degli investimenti per adattare i sistemi di comunicazione, dei costi di divulgazione dei dati alle autorità di contrasto e dei costi indotti dalle misure di sicurezza. È necessaria una visione globale per evitare eventuali effetti negativi sul livello di protezione dei dati e della sfera economica dei cittadini, cui potrebbe essere addebitata parte dei costi sostenuti dai fornitori. In questo contesto, si potrebbe anche considerare l'eventualità di subordinare il diritto del fornitore al rimborso dei costi al rispetto degli standard minimi e se tale diritto debba essere riconosciuto caso per caso.

Il gruppo è certo che le considerazioni esposte nel presente parere saranno tenute in debito conto e ricorda che è necessario porre in essere tutte le garanzie di cui sopra prima che entrino in vigore gli obblighi di conservazione dei dati.

Fatto a Bruxelles, il 21 ottobre 2005

Per il gruppo

Il presidente

Peter Schaar