I

(Risoluzioni, raccomandazioni e pareri)

PARERI

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del Garante europeo della protezione dei dati sulla neutralità della rete, la gestione del traffico e la protezione della vita privata e dei dati personali

(2012/C 34/01)

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]),

visto il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati ([2]), in particolare l'articolo 41, paragrafo 2,

vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche ([3]),

HA ADOTTATO IL SEGUENTE PARERE:

I. **INTRODUZIONE**

I.1. **Contesto**

1. Il 19 aprile 2011 la Commissione ha adottato una comunicazione sull'apertura e la neutralità della rete Internet in Europa ([4]).

2. Il presente parere può essere considerato la reazione del GEPD a tale comunicazione e mira a contribuire al dibattito politico in corso nell'Unione europea sulla neutralità della rete, in particolare sugli aspetti relativi alla protezione dei dati e della vita privata.

([1]) GU L 281 del 23.11.1995, pag. 31, la «direttiva sulla protezione dei dati personali».
([2]) GU L 8 del 12.1.2001, pag. 1, il «regolamento sulla protezione dei dati».
([3]) GU L 201 del 31.7.2002, pag. 37, modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 (cfr. nota 15), la «direttiva e-privacy».
([4]) COM(2011) 222 definitivo.

3. Il parere si basa sulla risposta ([5]) del GEPD alla consultazione pubblica della Commissione sull'apertura e la neutralità della rete Internet in Europa, che ha preceduto la comunicazione della Commissione. Il GEPD ha anche preso atto del recente progetto di conclusioni del Consiglio sulla neutralità della rete ([6]).

I.2. **Il concetto di neutralità della rete**

4. La neutralità della rete fa riferimento a un dibattito in corso sull'opportunità o meno di permettere che i fornitori di servizi Internet [ISP ([7])] limitino, filtrino o blocchino l'accesso a Internet o influiscano altrimenti sulle sue prestazioni. Il concetto di neutralità della rete si fonda sull'idea che in Internet le informazioni debbano essere trasmesse in modo imparziale, indipendentemente dal loro contenuto, dalla destinazione o dalla fonte, e che gli utenti debbano poter decidere quali applicazioni, servizi e hardware intendano usare. Questo significa che gli ISP non possono, a loro discrezione, definire priorità per l'accesso o rallentarlo per determinate applicazioni o servizi come il *peer to peer* (P2P) e simili ([8]).

5. Il filtraggio, il blocco e il controllo del traffico di rete sollevano questioni importanti, spesso trascurate o messe in secondo piano, che riguardano la riservatezza delle comunicazioni e il rispetto della vita privata delle persone fisiche e dei loro dati personali, quando usano Internet. Per esempio, determinate tecniche di controllo comportano il monitoraggio del contenuto delle comunicazioni, dei siti visitati, delle e-mail inviate e ricevute, degli orari in cui queste operazioni avvengono e simili, permettendo di filtrare le comunicazioni.

6. Controllando i dati delle comunicazioni, gli ISP potrebbero violarne la riservatezza, che è un diritto fondamentale garantito dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) e dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. La riservatezza è inoltre tutelata nella legislazione derivata dell'Unione europea, in particolare dall'articolo 5 della direttiva e-privacy.

I.3. **Obiettivo e struttura del parere**

7. Il GEPD ritiene che un serio dibattito politico sulla neutralità della rete debba occuparsi della riservatezza delle comunicazioni e delle altre conseguenze per la protezione dei dati e della vita privata.

8. Il presente parere contribuisce al dibattito in corso a livello di Unione europea. Il suo obiettivo è triplice:

— pone in risalto l'attinenza della protezione dei dati e della vita privata nelle attuali discussioni sulla neutralità della rete, sottolineando in particolar modo la necessità di rispettare le norme vigenti in materia di riservatezza delle comunicazioni. Devono essere ammesse solo le pratiche che rispettano tali norme,

— la neutralità della rete riguarda possibilità (tecnologiche) relativamente nuove e l'esperienza circa le modalità di applicazione del quadro giuridico è scarsa. Il presente parere fornisce pertanto un orientamento su come gli ISP debbano applicare e rispettare il quadro giuridico sulla protezione dei dati se si impegnano a filtrare, bloccare e controllare il traffico di rete. Ciò dovrebbe essere utile per gli ISP e anche per le autorità incaricate di attuare il quadro,

— nell'ambito della protezione dei dati e della vita privata, il presente parere identifica settori ai quali è necessario rivolgere particolare attenzione e che possono richiedere interventi da parte dell'Unione europea. Ciò è particolarmente importante alla luce del dibattito in corso a livello europeo e delle misure di politica che la Commissione potrebbe adottare in tale contesto.

([5]) Il GEPD ha risposto sottolineando quanto sia importante tenere conto delle questioni attinenti alla protezione dei dati e della vita privata, nonché degli altri valori e diritti esistenti. La risposta è consultabile all'indirizzo: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Consultabile all'indirizzo http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Tra questi servizi è inclusa la fornitura dell'accesso fisso e mobile a Internet.

([8]) Sebbene il principio non si applichi agli ISP che pongono limiti alla velocità o alla quantità di informazioni che un abbonato può inviare o ricevere mediante abbonamenti che prevedono limiti di larghezza di banda o di volume. Pertanto, applicando il principio di neutralità della rete, gli ISP potrebbero comunque offrire abbonamenti per l'accesso a Internet che limitano l'accesso in base a criteri come la velocità o il volume, purché non vi siano discriminazioni a favore o contro particolari contenuti.

9. Il GEPD è consapevole che la neutralità della rete solleva altre questioni, descritte più dettagliatamente qui di seguito, come quelle relative all'accesso alle informazioni. Tali questioni vengono affrontate soltanto per il motivo che sono collegate alla protezione dei dati e alla vita privata o vi influiscono.

10. Il parere è così strutturato: la sezione II inizia con una breve rassegna delle pratiche di filtraggio degli ISP. La sezione III delinea il quadro normativo dell'Unione europea in materia di neutralità della rete, mentre la sezione IV presenta una descrizione tecnica, seguita da una valutazione delle conseguenze per la vita privata a seconda della tecnologia utilizzata. La sezione V analizza i dettagli pratici riguardanti l'applicazione del quadro europeo attuale in materia di protezione dei dati e della vita privata. La sezione VI, basandosi su tale analisi, contiene suggerimenti per gli sviluppi politici futuri e individua i settori in cui potrebbe essere necessario chiarire e migliorare il quadro normativo. La sezione VII contiene le conclusioni.

II. **POLITICHE IN MATERIA DI NEUTRALITÀ DELLA RETE E GESTIONE DEL TRAFFICO**

Impiego crescente di politiche in materia di gestione del traffico

11. Tradizionalmente, gli ISP si sono impegnati a monitorare il traffico di rete e a influenzarlo soltanto in casi limitati. Per esempio, gli ISP hanno applicato tecniche di controllo e ridotto i flussi di informazioni per salvaguardare la sicurezza della rete, vale a dire per combattere i virus. Pertanto, in generale, Internet è cresciuta conservando un grado elevato di neutralità.

12. Tuttavia, negli ultimi anni, alcuni ISP hanno mostrato interesse per il controllo del traffico di rete al fine di differenziare e applicare politiche diverse, per esempio per bloccare servizi specifici o dare accesso preferenziale ad altri. Si tratta di quelle che talvolta sono definite «politiche di gestione del traffico» ([9]).

13. I motivi per cui gli ISP controllano e differenziano il traffico sono molteplici. Per esempio, le politiche di gestione del traffico possono servire agli ISP per regolare il traffico durante periodi di congestione elevata, dando la priorità ad alcuni tipi di traffico in tempo reale come il *video streaming* a scapito di altri generi di traffico nei quali il fattore tempo può essere meno importante, come il P2P ([10]). Inoltre, per gli ISP la gestione del traffico può essere un mezzo per ottenere un flusso potenziale di entrate da fonti diverse. D'altro canto, gli ISP potrebbero richiedere il pagamento di un importo ai fornitori di servizi di contenuti, per esempio quelli i cui servizi richiedono l'impiego di una larghezza di banda più elevata in cambio della priorità a loro accordata (e quindi di una maggiore velocità). Ciò significherebbe che l'accesso a un determinato servizio, per esempio un servizio di fornitura di *video on demand*, sarebbe più rapido dell'accesso a un altro servizio analogo per il quale non è stata acquistata la trasmissione ad alta velocità. Sarebbe possibile ottenere proventi anche dagli abbonati disposti a pagare importi maggiori (o inferiori) per alcuni tipi di abbonamenti differenziati. Per esempio, un abbonamento senza l'accesso al P2P potrebbe essere più economico di uno che dia diritto all'accesso illimitato.

14. Oltre ai motivi per cui gli ISP si avvalgono di politiche per la gestione del traffico, anche altre parti potrebbero essere interessate al fatto che gli ISP applichino tali politiche. Se questi ultimi gestiscono le loro reti e controllano i contenuti che passano attraverso le loro infrastrutture, è probabile che aumentino la loro capacità di individuare presunti utilizzi illeciti, per esempio la violazione dei diritti d'autore o la pornografia.

([9]) Cfr., per esempio, la relazione dell'OFCOM «Site blocking to reduce online copyright infringement», adottata il 27 maggio 2011 e disponibile all'indirizzo http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf in cui si afferma che alcuni ISP impiegano già sistemi di filtraggio dei pacchetti nella loro rete per la gestione del traffico e per altri scopi, per cui si ritiene che possa essere utilizzata l'ispezione approfondita dei pacchetti, anche se comporterebbe un elevato livello di complessità e di costi per coloro che ancora non usufruiscono di questi servizi. È possibile che nel breve o nel medio termine l'ispezione approfondita dei pacchetti possa essere impiegata soltanto dai maggiori ISP tenuto conto dell'investimento di capitali richiesto.

([10]) La qualità delle applicazioni in tempo reale come il *video streaming* dipende, tra l'altro, dalla latenza, ovvero dal ritardo dovuto, per esempio, alla congestione della rete.

Altri interessi in gioco, tra cui la protezione dei dati e della vita privata

15. Tale tendenza ha suscitato un dibattito sulla legittimità di questo genere di pratiche e soprattutto sulla necessità o meno di stabilire per legge ulteriori obblighi specifici in materia di neutralità della rete.

16. L'uso crescente da parte degli ISP di politiche per la gestione del traffico potrebbe limitare l'accesso alle informazioni. Se questo comportamento divenisse una prassi comune e se per gli utenti non fosse possibile (o fosse particolarmente costoso) avere un accesso a tutta la rete Internet come la conosciamo, si metterebbe a repentaglio l'accesso alle informazioni e la possibilità per l'utente di inviare e ricevere i contenuti desiderati utilizzando le applicazioni o i servizi che preferisce. Un principio giuridicamente vincolante relativo alla neutralità della rete potrebbe scongiurare questo problema.

17. Il GEPD è indotto quindi a considerare le conseguenze per la protezione dei dati e della vita privata quando gli ISP gestiscono il traffico. In particolare:

— quando gli ISP trattano i dati sul traffico al solo scopo di instradare il flusso di informazioni dal mittente al destinatario, in genere effettuano un trattamento limitato dei dati personali ([11]). Come il servizio postale tratta le informazioni presenti sulla busta di una lettera, l'ISP tratta le informazioni necessarie per instradare la comunicazione verso il destinatario. Ciò non è in contrasto con i requisiti giuridici della protezione dei dati, della vita privata e della riservatezza delle comunicazioni,

— tuttavia, quando gli ISP controllano i dati delle comunicazioni per differenziare ciascun flusso e applicare politiche specifiche che possono risultare pregiudizievoli per le persone fisiche, le conseguenze sono più rilevanti. A seconda delle circostanze di ogni caso e del tipo di analisi effettuata, il trattamento può essere molto invadente per quanto riguarda la vita privata e i dati personali. Ciò è ancora più ovvio quando le politiche di gestione rivelano il contenuto delle comunicazioni effettuate tramite Internet, tra cui le e-mail inviate e ricevute, i siti visitati, i file scaricati o caricati e così via.

III. PANORAMICA DEL QUADRO GIURIDICO DELL'UNIONE EUROPEA SULLA NEUTRALITÀ DELLA RETE E ULTERIORI SVILUPPI POLITICI

III.1. Il quadro giuridico in sintesi

18. Fino al 2009, gli strumenti normativi europei non contenevano disposizioni che vietassero espressamente agli ISP di filtrare o bloccare l'accesso ai servizi o di addebitare costi aggiuntivi agli abbonati a tali servizi, né contenevano disposizioni che riconoscessero esplicitamente questa pratica. La situazione non era chiaramente definita.

19. Il pacchetto Telecom del 2009 ha cambiato la situazione includendo disposizioni che favorivano l'apertura di Internet. Per esempio, l'articolo 8, paragrafo 4 del quadro normativo comune per le reti ed i servizi di comunicazione («direttiva quadro») impone alle autorità di regolamentazione di promuovere la capacità degli utenti finali di accedere a contenuti, applicazioni o servizi di loro scelta ([12]). Questa disposizione si applica a tutta la rete, non a livello di singoli fornitori di servizi. Inoltre, un recente progetto di conclusioni del Consiglio ha sottolineato la necessità di mantenere l'apertura di Internet ([13]).

([11]) Sono escluse attività volte ad aumentare la sicurezza della rete e rilevare il traffico nocivo, nonché operazioni necessarie per la fatturazione e l'interconnessione. Per questo trattamento sono inoltre esclusi gli obblighi derivanti dalla direttiva sulla conservazione dei dati, ovvero la 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) («direttiva sulla conservazione dei dati»).

([12]) Direttiva 2002/21/CE, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, modificata dalla direttiva 2009/140/CE e dal regolamento (CE) n. 544/2009 (GU L 337 del 18.12.2009, pag. 37).

([13]) Cfr. punto 3, lettera e), in cui il Consiglio riconosce la necessità di mantenere l'apertura di Internet, assicurando nel contempo che possa continuare a fornire servizi di elevata qualità in un contesto che promuova e rispetti diritti fondamentali quali la libertà di espressione e la libertà di esercitare un'attività, e punto 8, lettera d), che invita gli Stati membri a promuovere, quale loro obiettivo politico, l'apertura e la neutralità di Internet.

20. La direttiva servizio universale ([14]) prevede obblighi più concreti. Gli articoli 20 e 21 stabiliscono requisiti di trasparenza riguardanti le limitazioni all'accesso e/o all'utilizzo di servizi e applicazioni, nonché livelli minimi di qualità del servizio.

21. Per quanto riguarda le pratiche degli ISP che comportano il controllo delle comunicazioni tra persone fisiche, il considerando 28 della direttiva recante modifica della direttiva servizio universale e della direttiva e-privacy ([15]) sottolinea che «a seconda della tecnologia impiegata e del tipo di limitazione, tali limitazioni possono richiedere il consenso dell'interessato a norma della direttiva relativa alla vita privata e alle comunicazioni elettroniche». Pertanto, il considerando 28 ribadisce la necessità del consenso ai sensi dell'articolo 5, paragrafo 1, della direttiva e-privacy per qualsiasi limitazione effettuata sotto forma di sorveglianza delle comunicazioni. La sezione IV infra analizza ulteriormente l'applicazione dell'articolo 5, paragrafo 1 e il quadro giuridico globale in materia di protezione dei dati e della vita privata.

22. Infine, l'articolo 22, paragrafo 3, della direttiva servizio universale autorizza le autorità nazionali di regolamentazione a imporre agli ISP, ove necessario, prescrizioni in materia di qualità minima del servizio per impedire il degrado dei servizi e la limitazione o il rallentamento del traffico sulle reti pubbliche.

23. Quanto sopra esposto significa che, a livello di Unione europea, si riscontra una chiara aspirazione a una rete Internet aperta (cfr. articolo 8, paragrafo 4, della direttiva quadro). Tuttavia l'obiettivo di questa politica, che si applica all'intera rete, non riguarda direttamente divieti od obblighi per i singoli ISP. In altre parole, un ISP potrebbe attuare politiche di gestione del traffico, con la possibilità di escludere l'accesso a talune applicazioni, purché gli utenti finali siano pienamente informati e abbiano espresso il loro consenso liberamente, in modo specifico e inequivocabile.

24. La situazione può presentare aspetti differenti a seconda degli Stati membri. In alcuni di essi gli ISP possono, a determinate condizioni, adottare politiche di gestione del traffico, per esempio, per bloccare applicazioni come il VoIP (nell'ambito di un abbonamento a Internet a prezzo inferiore), a patto che le persone interessate abbiano dato liberamente, in modo specifico e inequivocabile il loro consenso informato. Altri Stati membri hanno deciso di rafforzare il principio di neutralità della rete. Per esempio, nel luglio 2011 il parlamento olandese ha varato una legge che vieta in generale ai provider di limitare o rallentare le applicazioni o i servizi in Internet (come il VoIP), a meno che ciò non sia necessario per ridurre al minimo gli effetti della congestione, per motivi di integrità o di sicurezza, per impedire lo *spam* o in seguito alla sentenza di un tribunale ([16]).

III.2. **La comunicazione sulla neutralità della rete**

25. Nella sua comunicazione sulla neutralità della rete ([17]), la Commissione europea ha concluso che la situazione della neutralità della rete deve essere monitorata e ulteriormente esaminata. La sua politica è stata ribattezzata «attendista», in quanto prende tempo per considerare ulteriori misure normative.

([14]) Direttiva 2002/22/CE, modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori (GU L 337 del 18.12.2009, pag. 11). Confronta anche l'articolo 1, paragrafo 3, in base a cui la direttiva, pur non prescrivendo né vietando agli ISP di limitare l'accesso e/o l'utilizzo di servizi e applicazioni da parte degli utenti finali, ove consentito dalla legislazione nazionale e in conformità al diritto comunitario, prevede tuttavia un obbligo di fornire informazioni in ordine a tali condizioni.

([15]) Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.

([16]) L'emendamento originale olandese è reperibile all'indirizzo https://zoek.officielebekendmakingen.nl/kst-32549-A.html. Nelle motivazioni riportate dalla stampa per questa scelta politica non si accennava a considerazioni sulla protezione dei dati e sulla vita privata, bensì alla necessità di garantire che gli utenti non venissero privati dell'accesso alle informazioni né che tale accesso venisse loro offerto in forma limitata. Sembra pertanto che l'emendamento sia stato motivato da questioni riguardanti l'accesso alle informazioni.

([17]) Cfr. nota 4.

26. In base alla comunicazione della Commissione, qualsiasi misura e qualsiasi ulteriore provvedimento normativo verranno sottoposti a una valutazione approfondita degli aspetti relativi alla protezione dei dati e alla vita privata. Il progetto di conclusioni del Consiglio accenna inoltre ai temi in gioco che riguardano la protezione dei dati e la vita privata ([18]).

27. Ciò che occorre valutare dal punto di vista della protezione dei dati e della vita privata è se una politica attendista sia sufficiente oppure no. Sebbene il quadro in materia di protezione dei dati e della vita privata preveda attualmente alcune clausole di salvaguardia, soprattutto in virtù del principio di riservatezza delle comunicazioni, risulta necessario monitorare da vicino il livello di conformità e l'orientamento in merito a diversi aspetti che non sono particolarmente chiari. Inoltre, vanno fatte alcune considerazioni su come semplificare e migliorare ulteriormente il quadro alla luce degli sviluppi tecnologici. Se il monitoraggio rivela un'evoluzione del mercato verso un controllo massiccio e in tempo reale delle comunicazioni e delle questioni relative alla conformità al quadro, si renderanno necessarie misure legislative. A questo proposito, nella sezione VI saranno forniti suggerimenti concreti.

IV. **CONTESTO TECNICO E RELATIVE CONSEGUENZE PER LA PROTEZIONE DEI DATI E DELLA VITA PRIVATA**

28. Prima di approfondire l'argomento, è importante avere un'idea più chiara delle tecniche di controllo che possono essere utilizzate dagli ISP per gestire il traffico e degli effetti che possono avere sul principio della neutralità della rete. Le conseguenze per la protezione dei dati e della vita privata derivanti da tali tecniche variano sensibilmente in base alla tecnica o alle tecniche impiegate. Questo contesto tecnico è necessario per comprendere e applicare correttamente il quadro giuridico in materia di protezione dei dati descritto nella sezione V. Tuttavia, occorre sottolineare che questo settore è complesso e costantemente in evoluzione, pertanto la descrizione che segue non intende essere esaustiva né pienamente aggiornata, ma soltanto fornire le informazioni di carattere tecnico che sono indispensabili per comprendere le motivazioni giuridiche.

IV.1. **La trasmissione di informazioni attraverso Internet: i fondamenti**

29. Quando un utente trasmette una comunicazione via Internet, le informazioni inviate vengono divise in pacchetti. I pacchetti vengono trasmessi attraverso Internet dal mittente al destinatario e ciascuno di essi include, tra gli altri, informazioni sulla fonte e sulla destinazione. Inoltre gli ISP possono incapsulare i pacchetti in ulteriori strati e protocolli ([19]), che vengono impiegati per gestire i diversi flussi di traffico all'interno della rete ISP.

30. Riallacciandosi alla similitudine con le lettere postali, utilizzare un protocollo di trasmissione di rete equivale a inserire una lettera tradizionale in una busta recante l'indirizzo del destinatario da far leggere al servizio postale, che successivamente consegna la busta. Il servizio postale può utilizzare protocolli aggiuntivi nell'ambito dei suoi transiti interni per gestire tutte le buste da trasmettere affinché ogni busta raggiunga la propria destinazione originariamente specificata dal mittente. In base a questa similitudine, ciascun pacchetto consta di due parti, il *payload IP* che include il contenuto della comunicazione, equivale alla lettera e contiene informazioni che sono indirizzate soltanto al destinatario. La seconda parte del pacchetto è l'*header IP*, che comprende, tra gli altri, gli indirizzi del destinatario e del mittente ed equivale alla busta. L'*header IP* consente agli ISP e ad altri intermediari di inoltrare il *payload* dall'indirizzo di partenza al suo indirizzo di destinazione.

31. Gli ISP e gli altri intermediari garantiscono che i pacchetti IP viaggino nella rete attraverso nodi che leggono le informazioni dell'*header IP*, le controllano facendo riferimento a tabelle di instradamento (*routing tables*) e poi le inoltrano al nodo successivo lungo il percorso che porta alla destinazione. Questo processo avviene attraverso la rete utilizzando un approccio «per quanto possibile senza

([18]) Cfr. punto 4, lettera e), in cui il Consiglio constata l'esistenza di alcune questioni riguardanti la protezione dei dati personali, sollevate principalmente dai consumatori e dalle autorità garanti della protezione dei dati.

([19]) Come descritto più dettagliatamente nella sezione IV.2, questi protocolli (tra i quali HTTP, FTP e simili) codificano le informazioni trasmesse da punto a punto secondo una modalità concordata affinché i dispositivi coinvolti nella comunicazione possano comprendersi reciprocamente.

memoria», dal momento che tutti i pacchetti che pervengono a un nodo vengono trattati in modo neutrale. Quando vengono inoltrati al nodo successivo non occorre conservare ulteriori informazioni nel *router* ([20]).

IV.2. **Tecnologie di controllo**

32. Come menzionato in precedenza, gli ISP leggono gli *header IP* allo scopo di instradarli verso la loro destinazione. Tuttavia, si è accennato al fatto che l'analisi del traffico (che coinvolge gli *header IP* e i *payload IP*) può essere effettuata per altri scopi e con tipi di tecnologie diversi. Tra le nuove tendenze figurano, per esempio, il rallentamento di determinate applicazioni utilizzate dagli utenti, per esempio il P2P, o in alternativa l'aumento della velocità del traffico per taluni servizi come il *video on demand* per gli abbonati *premium*. Benché tutte le tecnologie di controllo eseguano tecnicamente l'ispezione del pacchetto, i livelli di invadenza che comportano sono differenti. Se ne distinguono due categorie principali: una si basa soltanto sull'*header IP*, l'altra anche sul *payload IP*.

Informazioni basate sull'header IP. Il controllo dell'*header IP* di un pacchetto rivela alcuni campi che possono consentire agli ISP di applicare una serie di politiche specifiche per gestire il traffico. Tali tecnologie basate esclusivamente sul controllo degli *header IP* trattano per finalità diverse (per esempio la differenziazione del traffico) dati che in linea di principio servono a instradare le informazioni. Esaminando l'indirizzo IP sorgente, l'ISP può associarlo a un preciso abbonato e applicare politiche specifiche, per esempio instradando il pacchetto attraverso un link più veloce o più lento. L'ISP può adottare politiche specifiche anche vedendo l'indirizzo IP di destinazione, per esempio bloccando o filtrando l'accesso a determinati siti web.

Tecnologie basate su un controllo più approfondito. L'ispezione più approfondita di un pacchetto di dati permette all'ISP di accedere alle informazioni indirizzate esclusivamente al destinatario della comunicazione. Riprendendo l'esempio del servizio postale, questo approccio equivale ad aprire la busta e a leggere la lettera per eseguire un'analisi del contenuto della comunicazione (che è incapsulato nei pacchetti IP) al fine di applicare una politica di rete specifica. Ci sono diversi modi per effettuare il controllo e ciascuno di essi comporta minacce diverse per le persone interessate dai dati.

— *Ispezione approfondita dei pacchetti di dati basata sull'analisi di protocolli e su dati statistici.* Oltre al protocollo IP, il cui scopo è permettere la trasmissione dei dati via Internet, esistono protocolli aggiuntivi che codificano le informazioni trasmesse secondo una modalità concordata (trasporto, sessione, presentazione e applicazione, e così via). Obiettivo di questi protocolli è garantire che le parti interessate alla comunicazione possano comprendersi reciprocamente. Esistono per esempio protocolli impiegati per navigare in Internet ([21]), altri servono per trasferire file ([22]) e simili. Le tecnologie di controllo basate sull'ispezione dei protocolli e combinate con analisi statistiche sono dunque volte a rilevare modelli specifici o caratteristiche che determinano quali protocolli sono presenti ([23]). Queste tecnologie di controllo permettono agli ISP di comprendere il tipo di comunicazione (e-mail, navigazione in rete, caricamento di file) e, in alcuni casi, di identificare l'applicazione o il servizio specifico utilizzati, come nel caso di alcune comunicazioni VoIP in cui i protocolli impiegati sono molto specifici per un determinato rivenditore o fornitore di servizi. Di per sé il fatto di conoscere il tipo di comunicazione può permettere agli ISP di applicare politiche concrete di gestione del traffico, per esempio, per bloccare il traffico di rete. Può trattarsi anche del primo passo per consentire all'ISP di eseguire ulteriori analisi che potrebbero richiedere il pieno accesso ai metadati e al contenuto della comunicazione.

([20]) Tuttavia, i dispositivi della rete Internet utilizzano protocolli di instradamento che registrano le attività, le statistiche del traffico di processo e scambiano informazioni con altri dispositivi di rete per instradare i pacchetti IP utilizzando il percorso più efficace. Per esempio, quando un link è congestionato o interrotto e un *router* riceve quest'informazione, esso aggiornerà la propria tabella di instradamento con un percorso alternativo che non contiene quel link. Inoltre, va sottolineato che in alcuni casi la raccolta e il trattamento possono essere effettuati a scopi di fatturazione oppure anche in conformità alle prescrizioni della direttiva sulla conservazione dei dati.

([21]) HTTP — Hypertext transfer protocol — oppure HTML — Hypertext Markup Language.

([22]) FTP — File transfer protocol.

([23]) Ci sono diversi modi per individuare i protocolli utilizzati. Per esempio è possibile cercare protocolli interni in campi specifici per identificare le porte utilizzate per stabilire la comunicazione, dal cui flusso si possono ricavare dati statistici tramite l'analisi di alcuni campi specifici e la correlazione dei protocolli impiegati simultaneamente tra due indirizzi IP.

— *Ispezione approfondita dei pacchetti di dati basata sull'analisi del contenuto della comunicazione.* Infine, è possibile anche verificare i metadati ([24]) e il contenuto stesso della comunicazione. Questa tecnologia consiste nell'intercettare tutti i pacchetti IP che fanno parte del flusso originale della comunicazione, in modo da poter ricostruire pienamente e analizzare il contenuto originale della comunicazione. Ad esempio, per rilevare la presenza di contenuti nocivi o illegali come virus, pedopornografia, e simili, è necessario ricostruire il contenuto stesso della comunicazione per poterlo analizzare. Occorre osservare che talvolta la comunicazione può essere esplicitamente e completamente criptata dalle parti interessate e questa pratica impedisce agli ISP di effettuare l'analisi del suo contenuto.

IV.3. **Conseguenze per la protezione della vita privata e dei dati**

33. Le tecnologie di controllo basate sugli *header IP* e, in particolare, sull'ispezione dei pacchetti, comportano il monitoraggio e il filtraggio dei dati e hanno gravi conseguenze per la protezione della vita privata e dei dati. Inoltre possono essere incompatibili con il diritto alla riservatezza delle comunicazioni.

34. Il fatto di leggere le comunicazioni delle persone comporta di per sé gravi conseguenze per la protezione della vita privata e dei dati. Eppure, il problema è più ampio in quanto, a seconda degli effetti dovuti al monitoraggio e all'intercettazione, le conseguenze per la vita privata possono rivelarsi ancora più numerose. Infatti, limitarsi a controllare le comunicazioni, per esempio, solo per garantire che il sistema funzioni bene non è lo stesso che controllarle per applicare politiche che possono avere un impatto sulle persone fisiche. Quando le politiche riguardanti il traffico e le scelte mirano soltanto a evitare la congestione della rete, non ci sono gravi conseguenze per la vita privata delle persone. Tuttavia, le politiche di gestione del traffico possono avere lo scopo di bloccare alcune informazioni sul contenuto o influire sulla comunicazione, per esempio con la pubblicità comportamentale. In questo caso gli effetti sono più invasivi. La questione diventa più critica se ci si rende conto che questo tipo di informazioni verrebbe raccolto non in relazione a un piccolo gruppo di persone, bensì su base generale, comprendendo tutti i clienti degli ISP ([25]). Se tutti gli ISP adottassero tecniche di filtraggio, ciò potrebbe comportare un monitoraggio generalizzato della navigazione in Internet. Inoltre, se ci si concentra sul tipo di informazioni trattate, i rischi per la vita privata sono ovviamente elevati, perché molte delle informazioni che vengono raccolte potrebbero essere molto sensibili e, una volta raccolte, sarebbero a disposizione degli ISP e di chi volesse richiedergliele. Inoltre, le informazioni potrebbero essere molto preziose sotto l'aspetto commerciale. Questo è in sé un grave rischio di *function creep*, in cui gli obiettivi iniziali potrebbero facilmente trasformarsi nello sfruttamento commerciale, o di altro tipo, delle informazioni raccolte.

35. L'applicazione corretta delle tecnologie di monitoraggio, controllo e filtraggio deve avvenire in conformità alle clausole di salvaguardia sulla protezione dei dati e sulla vita privata, che stabiliscono limiti riguardo a ciò che si può fare e in quali circostanze. Nella prossima sezione viene fornita una panoramica delle clausole di salvaguarda applicabili in base all'attuale quadro giuridico europeo in materia di protezione dei dati e sulla vita privata.

V. **APPLICAZIONE DEL QUADRO GIURIDICO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI E DELLA VITA PRIVATA**

36. Il quadro normativo europeo in materia di protezione dei dati è neutrale per quanto riguarda le tecnologie e, come tale, non disciplina quelle specifiche di controllo descritte in precedenza. La direttiva e-privacy disciplina il rispetto della vita privata nell'offerta di servizi di comunicazione elettronica nelle

([24]) Ogni protocollo ha nel proprio *header* alcuni campi specifici che forniscono informazioni aggiuntive di carattere informale sulla comunicazione in corso di trasmissione. Pertanto i contenuti di questi campi possono essere definiti i metadati della comunicazione. Un esempio di questi campi è il numero di porta usato: se è il numero 80, è molto probabile che il tipo di comunicazione sia *web browsing*.

([25]) Naturalmente le possibilità di tracciamento non sono esclusive degli ISP. Anche i *provider* di reti di inserzioni sono in grado, tramite l'impiego di *cookie* di terzi, di tracciare gli utenti dei siti. Cfr., per esempio, un recente articolo accademico che dimostra la presenza di Google in 97 dei 100 principali siti Internet: ciò significa che Google può tracciare gli utenti che non hanno selezionato l'opzione di *opt out* relativa ai *cookie* di terzi quando navigano su questi siti popolari. Cfr.: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan e Hoofnagle, Chris Jay, Flash Cookies e Privacy II: attualmente con HTML5 e ETag Respawning (29 luglio 2011). Disponibile sul sito di SSRN: (http://ssrn.com/abstract=1898390). Il tracciamento degli utenti mediante i *cookie* di terzi è stato affrontato dal Gruppo di lavoro «articolo 29». Cfr. parere 2/2010 sulla pubblicità comportamentale *on line* adottato il 22 giugno 2010 (WP 171).

reti pubbliche (in particolare l'accesso a Internet e la telefonia) ([26]) e la direttiva sulla protezione dei dati personali disciplina il trattamento dei dati in generale. Considerato nel suo complesso, questo quadro giuridico stabilisce diversi obblighi che si applicano agli ISP che trattano e monitorano i dati sul traffico e sulle comunicazioni.

V.1. **Basi giuridiche per il trattamento dei dati sul traffico e sui contenuti**

37. In base alla normativa sulla protezione dei dati, il trattamento dei dati personali, quali sono nel caso specifico i dati sul traffico e sulle comunicazioni, richiede una base giuridica adeguata. Oltre a questo requisito generale, in determinati casi si possono applicare requisiti specifici.

38. In questo caso, il tipo di dati personali che vengono trattati dagli ISP è costituito dai dati sul traffico e dal contenuto delle comunicazioni. Sia i primi che il secondo sono protetti dal diritto alla riservatezza della corrispondenza, garantito dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e dagli articoli 7 e 8 della Carta europea dei diritti fondamentali. In particolare, l'articolo 5, paragrafo 1 della direttiva e-privacy, intitolato «riservatezza delle comunicazioni» richiede agli Stati membri di assicurare la riservatezza delle comunicazioni e dei relativi dati sul traffico tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, prevedendo al contempo che il trattamento dei dati sul traffico e sul contenuto da parte degli ISP possa essere consentito, in determinate circostanze, previo consenso degli utenti, dal momento che la norma in questione vieta «l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1». Ciò viene ulteriormente esaminato in seguito.

39. Oltre al consenso degli utenti interessati, la direttiva e-privacy contempla altre ragioni che possono legittimare il trattamento dei dati sul traffico e sulla comunicazione ad opera degli ISP. In questo caso le basi giuridiche per il trattamento riguardano i) la fornitura del servizio, ii) la salvaguardia della sicurezza del servizio offerto e iii) la riduzione al minimo della congestione. Altre motivazioni possibili che legittimino le politiche di gestione basate sui dati sul traffico o sulle comunicazioni sono discussi infra al punto iv).

i) Basi giuridiche per la fornitura del servizio

40. Come illustrato nella sezione IV, gli ISP trattano le informazioni sugli *header IP* per instradare ogni pacchetto IP verso la sua destinazione. L'articolo 6, paragrafi 1 e 2, della direttiva e-privacy permette di trattare i dati sul traffico allo scopo di trasmettere la comunicazione. Pertanto, gli ISP possono trattare le informazioni necessarie per la fornitura del servizio.

ii) Basi giuridiche per la salvaguardia della sicurezza del servizio

41. Ai sensi dell'articolo 4 della direttiva e-privacy, un ISP è tenuto all'obbligo generale di prendere appropriate misure per salvaguardare la sicurezza dei suoi servizi. La pratica di filtrare i virus può comportare il trattamento degli *header IP* e dei *payload IP*. Considerando che l'articolo 4 della direttiva e-privacy richiede agli ISP di garantire la sicurezza della rete, questa disposizione legittima tecnologie di controllo basate sul contenuto e sugli *header IP* che mirino esclusivamente al conseguimento di questo fine. In pratica, ciò significa che, nei limiti stabiliti dal principio di proporzionalità (cfr. sezione V.3), gli ISP possono monitorare e filtrare i dati delle comunicazioni per combattere i virus e garantire in generale la sicurezza della rete ([27]).

([26]) Il considerando 10 della direttiva e-privacy afferma: «Nel settore delle comunicazioni elettroniche trova applicazione la direttiva 95/46/CE, in particolare per quanto riguarda tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali non specificatamente disciplinati dalle disposizioni della presente direttiva, compresi gli obblighi del responsabile e i diritti delle persone fisiche». Inoltre, il considerando 17 riguarda il consenso da parte delle persone interessate dai dati recita: «Ai fini della presente direttiva il consenso dell'utente o dell'abbonato, senza considerare se quest'ultimo sia una persona fisica o giuridica, dovrebbe avere lo stesso significato del consenso della persona interessata come definito ed ulteriormente determinato dalla direttiva 95/46/CE».

([27]) Parere 2/2006 del gruppo di lavoro «articolo 29» sugli aspetti della protezione della vita privata inerenti ai servizi di screening dei messaggi di posta elettronica, adottato il 21 febbraio 2006 (WP 118). In questo parere, il gruppo di lavoro ritiene che l'attivazione di filtri per gli scopi dell'articolo 4 possa essere compatibile con l'articolo 5 della direttiva e-privacy.

iii) Basi giuridiche per la riduzione al minimo degli effetti della congestione

42. La ragion d'essere di questa base giuridica è contenuta nel considerando 22 della direttiva e-privacy, che spiega il divieto di memorizzare le comunicazioni stabilito dall'articolo 5, paragrafo 1. Il divieto non riguarda eventuali memorizzazioni automatiche, intermedie e temporanee, a patto che vengano effettuate a scopo di trasmissione e non durino per un periodo superiore a quanto necessario per la trasmissione e ai fini della gestione del traffico e che sia assicurata la riservatezza delle comunicazioni.

43. In caso di congestione, si pone il problema della possibilità o meno per gli ISP di ritardare o interrompere casualmente il traffico o di rallentare le comunicazioni per le quali il fattore tempo è meno importante, come il P2P o le e-mail, consentendo, ad esempio, per il traffico vocale il passaggio a una qualità accettabile.

44. Considerato l'interesse generale della società per la garanzia di una rete di comunicazioni utilizzabile, gli ISP potrebbero sostenere che dare priorità al traffico o limitarlo per risolvere il problema della congestione è una misura legittima e indispensabile per fornire un servizio adeguato. Questo vuol dire che in tali casi e a questo scopo ci sarebbe una base giuridica generale per trattare i dati personali e non sarebbe più necessario il consenso specifico degli utenti.

45. Al tempo stesso, la possibilità di interferire in questo modo non è priva di restrizioni. Se gli ISP hanno bisogno di controllare le comunicazioni, sotto l'aspetto della riservatezza, e applicando rigorosamente il principio della proporzionalità, devono utilizzare il metodo meno invasivo disponibile per raggiungere lo scopo (evitando l'ispezione approfondita dei pacchetti di dati) e applicarlo solo per il tempo necessario per risolvere la congestione.

iv) Basi giuridiche per il trattamento dei dati per altri scopi

46. È possibile che gli ISP intendano controllare i dati sul traffico e sui contenuti per altri scopi, tra cui quello di offrire abbonamenti mirati (per esempio un abbonamento che limiti l'accesso al P2P o che aumenti la velocità di determinate applicazioni). Il controllo e l'ulteriore utilizzo dei dati sul traffico e sulle comunicazioni per scopi diversi dalla fornitura del servizio, dalla garanzia della sua sicurezza e dell'assenza di congestioni sono permessi soltanto a condizioni rigorose, in conformità al quadro giuridico.

47. Il quadro giuridico è rappresentato principalmente dall'articolo 5, paragrafo 1, della direttiva e-privacy che richiede il consenso degli utenti per l'ascolto, la captazione, la memorizzazione o altre forme di intercettazione e di sorveglianza delle comunicazioni e dei relativi dati sul traffico. In pratica questo significa che il consenso degli utenti che prendono parte a una comunicazione è necessario per legittimare il trattamento dei dati sul traffico e sulle comunicazioni, ai sensi dell'articolo 5, paragrafo 1.

48. Come spiegato in precedenza, l'applicazione delle tecnologie di controllo e di filtraggio è basata sugli *header IP*, ovvero i dati sul traffico, o sull'ispezione approfondita dei pacchetti di dati che riguarda anche i *payload IP*, vale a dire i dati sulla comunicazione. Pertanto, in linea di principio, l'applicazione di queste tecnologie per scopi diversi dalla trasmissione o dalla sicurezza del servizio sarebbe vietata, a meno che una ragione legittima, come il consenso, permetta il trattamento (articolo 5, paragrafo 1). Un esempio di applicazione di quest'articolo è il caso in cui un ISP decida di offrire ai clienti l'accesso a Internet a un prezzo ridotto in cambio della ricezione di pubblicità comportamentale, dell'utilizzo dell'ispezione approfondita dei pacchetti di dati e conseguentemente dei dati sulla comunicazione. Il consenso effettivo, specifico e informato si rende quindi necessario a norma dell'articolo 5, paragrafo 1.

49. Inoltre, l'articolo 6 della direttiva e-privacy, dal titolo «dati sul traffico», stabilisce alcune norme che si applicano appositamente ai dati sul traffico. In particolare, prevede la possibilità per gli ISP di trattare i

dati sul traffico, sempre che l'utente abbia dato il proprio consenso, per la fornitura di servizi a valore aggiunto ([28]). Questa disposizione specifica il requisito del consenso previsto dall'articolo 5, paragrafo 1, quando si tratta dei dati sul traffico.

50. In pratica, non è sempre facile stabilire in quali casi il consenso sia necessario e in quali altri la sicurezza della rete possa giustificare il trattamento, soprattutto se gli scopi delle tecnologie di controllo sono duplici (ad esempio, evitare la congestione e fornire servizi a valore aggiunto). Va sottolineato che il consenso non si può considerare una scorciatoia comoda e sistematica per ottenere la conformità ai principi su cui si fonda la protezione dei dati.

51. Scarsa è l'esperienza nell'applicazione del quadro, in particolare per quanto riguarda i vari aspetti descritti in precedenza. Si tratta di un settore in cui sono essenziali ulteriori orientamenti, come specificato nella sezione VI. Inoltre, esistono altri aspetti pertinenti, relativi all'ottenimento del consenso, che richiedono anch'essi una particolare considerazione e sono descritti di seguito.

V.2. **Aspetti relativi al consenso informato come base giuridica**

52. Il consenso richiesto in base agli articoli 5 e 6 della direttiva e-privacy ha lo stesso significato del consenso della persona interessata come definito e ulteriormente determinato nella direttiva 95/46/CE ([29]). In base all'articolo 2, lettera h), della direttiva sulla protezione dei dati personali, per «consenso della persona interessata» si intende «qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento». Recentemente il ruolo del consenso e i requisiti che ne determinano la validità sono stati affrontati dal gruppo di lavoro «articolo 29» nel suo parere 15/2011 sul consenso ([30]).

53. Gli ISP che richiedono il consenso per effettuare il controllo e il filtraggio dei dati sul traffico e sui contenuti devono pertanto accertarsi che il consenso sia libero e specifico e sia una manifestazione di volontà pienamente informata con la quale una persona fisica accetta che i dati personali che la riguardano siano oggetto di un trattamento. Il considerando 17 della direttiva e-privacy ribadisce tale concetto: «[…]. Il consenso può essere fornito secondo qualsiasi modalità appropriata che consenta all'utente di esprimere liberamente e in conoscenza di causa i suoi desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito Internet». Qui di seguito vengono forniti alcuni esempi pratici di cosa si intenda in tale contesto per consenso libero, specifico e informato.

Consenso: manifestazione di volontà libera, specifica e informata

54. *Consenso libero*. Gli utenti non devono essere soggetti a costrizioni per quanto riguarda il consenso all'abbonamento a Internet che intendono sottoscrivere.

55. Le persone non fornirebbero liberamente il loro consenso se, per ottenere l'accesso a un servizio di comunicazione, dovessero acconsentire a che i dati delle loro comunicazioni vengano monitorati. Ciò vale ancor più se tutti i provider in un determinato mercato gestissero il traffico per finalità che vanno al di là della sicurezza della rete. La sola opzione che resterebbe a disposizione degli utenti sarebbe quella di non abbonarsi affatto ai servizi Internet. Poiché la rete Internet è diventata uno strumento

([28]) Il considerando 18 della direttiva contiene un elenco di tali servizi a valore aggiunto. Non è chiaro se i servizi per i quali si attuano le politiche di gestione del traffico possano essere considerati parte dell'elenco. Le politiche di gestione del traffico volte a dare la priorità a determinati contenuti potrebbero essere intese come una qualità del servizio. Per esempio, una gestione del traffico che comporti soltanto il trattamento degli *header IP* e abbia per finalità quella di offrire videogiochi a prezzi particolarmente vantaggiosi, dando la priorità in rete al traffico degli utenti che ci stanno giocando, potrebbe essere considerata un valore aggiunto. D'altra parte, è lungi dall'essere chiaro se si possa definire così una gestione del traffico che limiti determinati tipi di traffico, per esempio quello P2P.

([29]) Cfr. considerando 17 e articolo 2, lettera f), della direttiva e-privacy.

([30]) Adottato il 13 luglio 2011 (WP 187).

essenziale sia per il lavoro che per lo svago, la scelta di non abbonarsi a un servizio Internet non costituisce una valida alternativa. Ne conseguirebbe che le persone non avrebbero una possibilità di scelta vera e propria, il che equivale a dire che non potrebbero fornire un consenso libero ([31]).

56. Il GEPD ritiene che per la Commissione e le autorità nazionali sia evidentemente necessario monitorare il mercato, soprattutto per stabilire se questa situazione — che vede i provider associare i servizi di telecomunicazione al monitoraggio delle comunicazioni — stia diventando la norma. I provider dovrebbero offrire servizi alternativi, compreso un abbonamento a Internet non soggetto alla gestione del traffico, senza imporre costi più elevati alle persone interessate.

57. *Consenso specifico*. L'esigenza di un consenso che sia specifico implica, in questo caso, che gli ISP lo richiedano in maniera chiara e distinta quando riguarda il monitoraggio dei dati sul traffico e sulle comunicazioni. Secondo il gruppo di lavoro «articolo 29», «… per essere specifico, il consenso dev'essere comprensibile: dovrebbe cioè riferirsi chiaramente e precisamente al campo di applicazione e alle conseguenze del trattamento dei dati. Non può riferirsi a un insieme illimitato di attività di trattamento. Ciò significa, in altre parole, che il contesto al quale si applica il consenso è limitato». Difficilmente si ottiene un consenso specifico se il consenso al controllo dei dati sul traffico e sulle comunicazioni viene «abbinato» al consenso generale riguardante l'abbonamento al servizio. La specificità implica invece l'utilizzo di mezzi mirati per ottenere il consenso, per esempio un modulo di consenso specifico o una casella separata da barrare che faccia chiaramente riferimento alla finalità del monitoraggio dei dati (anziché l'inclusione delle informazioni nelle condizioni generali del contratto e l'obbligo di firmarlo).

58. *Consenso informato*. Per essere valido, il consenso deve essere informato. La necessità di fornire informazioni preliminari adeguate deriva non solo dalla direttiva e-privacy e dalla direttiva sulla protezione dei dati, ma anche dagli articoli 20 e 21 della direttiva servizio universale, modificata dalla direttiva 2009/136/CE ([32]). Il fatto che le informazioni e il consenso siano necessari è stato espressamente confermato dal considerando 28 della direttiva 2009/136/CE: «gli utenti dovrebbero in ogni caso essere pienamente informati di qualsiasi condizione imposta dal fornitore di servizio e/o di rete che limita l'utilizzo di servizi di comunicazione elettronica. Tali informazioni dovrebbero, a discrezione del fornitore, specificare il tipo di contenuto, applicazione o servizio interessati, le single applicazioni o servizi, o entrambi». Lo stesso considerando specifica quindi che «a seconda della tecnologia impiegata e del tipo di limitazione, tali limitazioni possono richiedere il consenso dell'interessato a norma della direttiva 2002/58/CE».

59. Data la complessità delle tecnologie di monitoraggio, fornire informazioni preliminari pertinenti è uno dei principali presupposti per il conseguimento di un consenso valido. I consumatori dovrebbero essere informati in modo che possano comprendere quali dati vengono sottoposti a trattamento, come vengono utilizzati e gli effetti sull'esperienza dell'utente nonché il livello di invasività della vita privata che tali tecnologie comportano.

60. Ciò significa non solo che le informazioni devono essere chiare e comprensibili per l'utente medio, ma anche che devono essere fornite direttamente alle persone in modo palese, affinché non possano passare inosservate.

61. *Manifestazione della volontà*. In base al quadro giuridico applicabile, il consenso richiede inoltre un atto affermativo da parte dell'utente per manifestare la propria approvazione. Un consenso tacito non soddisferebbe questo criterio. Anche queste considerazioni confermano che è necessario impiegare mezzi mirati per ottenere un consenso che permetta all'ISP di controllare i dati sul traffico e sulle comunicazioni nel contesto dell'attuazione di politiche di gestione del traffico. Nel suo recente parere sul consenso, il gruppo di lavoro «articolo 29» ha sottolineato la necessità dell'articolazione del consenso per quanto concerne i vari elementi che costituiscono il trattamento dei dati.

([31]) Un caso analogo è stato riscontrato in merito alla registrazione dei nominativi dei passeggeri quando è stata dibattuta la validità o meno del consenso dei passeggeri a trasmettere i dati relativi alle prenotazioni alle autorità statunitensi. Il Gruppo di lavoro ha affermato che il consenso dei passeggeri non può essere fornito liberamente perché le compagnie aeree sono obbligate a trasmettere i dati prima della partenza del volo e i passeggeri non hanno quindi una reale possibilità di scelta se intendono viaggiare in aereo (parere 6/2002 del Gruppo di lavoro «articolo 29» relativo alla trasmissione da parte delle compagnie aeree di informazioni sugli elenchi dei passeggeri e di altri dati agli Stati Uniti).

([32]) Direttiva 2009/136/CE, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (cfr. nota 15).

62. Si potrebbe argomentare che, se le parti coinvolte in una comunicazione non vogliono che gli ISP la intercettino per attuare politiche di gestione del traffico, possono criptare la comunicazione. Questo approccio può essere considerato utile all'atto pratico, ma richiede un certo impegno e conoscenze tecniche e non può essere ritenuto analogo a un consenso libero, specifico e informato. Inoltre, l'utilizzo di tecniche di cifratura non salvaguarda pienamente la riservatezza di una comunicazione poiché l'ISP può accedere almeno alle informazioni sull'*header IP* per instradare la comunicazione e può anche effettuare analisi statistiche.

63. In base all'articolo 5, paragrafo 1, della direttiva e-privacy, il consenso deve essere accordato dagli utenti interessati. In molti casi l'utente coincide con l'abbonato, il quale accorda il suo consenso nel momento in cui si abbona al servizio di comunicazione. In altri casi, compresi quelli in cui può essere interessata più di una persona, il consenso degli utenti deve essere ottenuto separatamente, e questo fatto potrebbe sollevare alcune questioni pratiche, come di seguito descritte.

Consenso di tutti gli utenti interessati

64. L'articolo 5, paragrafo 1 prevede che il consenso dell'utente legittimi il trattamento. Il consenso deve essere accordato da tutti gli utenti interessati a una comunicazione. Il motivo è che di norma una comunicazione riguarda almeno due persone (il mittente e il destinatario). Per esempio, se un ISP esamina i *payload IP* relativi a una e-mail, le informazioni sottoposte a controllo riguardano sia il mittente che il destinatario della e-mail.

65. Durante il monitoraggio e l'intercettazione del traffico e delle comunicazioni (per esempio, di un certo tipo di traffico su Internet), per gli ISP può essere sufficiente ottenere il consenso dell'utente, ovvero dell'abbonato. Ciò dipende dal fatto che l'altra parte coinvolta nella comunicazione, in questo caso un sito Internet visitato, non può essere considerata un «utente interessato» ([33]). Tuttavia, la situazione può risultare più complessa quando il monitoraggio comporta il controllo del contenuto di e-mail e pertanto, delle informazioni personali del mittente e del destinatario di una e-mail, che potrebbero non avere un rapporto contrattuale con lo stesso ISP. In questi casi, l'ISP tratterebbe dati personali (nome, indirizzo della e-mail e dati del suo contenuto potenzialmente sensibili) di persone che non sono suoi clienti. Da un punto di vista pratico, ottenere il consenso di queste persone può rivelarsi più difficile, perché dovrebbe essere richiesto di volta in volta anziché all'atto della conclusione del servizio di telecomunicazione. Non sarebbe neppure realistico supporre che il consenso dell'abbonato venga dato anche a nome di altri utenti, come avviene spesso nel caso di privati in ambiente domestico.

66. In tale contesto, il GEPD ritiene che gli ISP debbano attenersi ai requisiti giuridici vigenti e attuare politiche che non comportano il monitoraggio e il controllo di informazioni. Questo aspetto è ancora più importante nel caso di servizi di comunicazione che coinvolgono terzi i quali non possono acconsentire al monitoraggio, e soprattutto nel caso di e-mail inviate e ricevute (ciò non si applica quando la finalità è legata a considerazioni di sicurezza).

67. Al contempo, va sottolineato che la normativa nazionale che recepisce l'articolo 5, paragrafo 1, della direttiva e-privacy non sempre può risultare soddisfacente a questo proposito, e che in generale sembrano necessari orientamenti più adeguati per quanto riguarda i requisiti della direttiva e-privacy in tale contesto. Il GEPD invita pertanto la Commissione a intervenire più attivamente al riguardo e a prendere un'iniziativa che potrebbe beneficiare del contributo delle autorità di vigilanza che partecipano alle riunioni del gruppo di lavoro «articolo 29» e di altre parti interessate. Se necessario, si dovrebbe adire la Corte di giustizia per fare piena chiarezza sul significato e sulle conseguenze dell'articolo 5, paragrafo 1.

([33]) Ciò vale anche nei casi in cui il traffico su Internet comporta il trasferimento di informazioni personali quali, per esempio, immagini di persone fisiche identificabili pubblicate su un sito Internet. Il trattamento di tali informazioni necessita di una base giuridica, ma non sarebbe contemplato dall'articolo 5, paragrafo 1, in quanto queste persone non sarebbero «utenti interessati».

V.3. **Proporzionalità — principio della minimizzazione dei dati**

68. L'articolo 6, lettera c) della direttiva sulla protezione dei dati sancisce il principio di proporzionalità ([34]), che si applica agli ISP in quanto controllori di dati ai sensi di questa direttiva, quando effettuano il monitoraggio e il filtraggio.

69. Secondo tale principio, i dati personali possono essere trattati soltanto se sono «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati». L'applicazione di questo principio comporta la necessità di effettuare una valutazione per determinare se i mezzi impiegati per il trattamento dei dati e i tipi di dati personali utilizzati sono adatti e se esiste la ragionevole possibilità che conseguano i loro obiettivi. Se la conclusione è che vengono raccolti più dati del necessario, il principio non è soddisfatto.

70. La conformità al principio di proporzionalità di determinati tipi di tecnologie di controllo deve essere valutata caso per caso. Non è possibile giungere a conclusioni in abstracto. Tuttavia, si possono indicare diversi aspetti concreti che dovrebbero essere presi in considerazione nel valutare il rispetto del principio di proporzionalità.

71. *La quantità di informazioni trattate.* Sorvegliare le comunicazioni dei clienti di un ISP nel modo più rigoroso possibile è, nella maggior parte dei casi, eccessivo e illegale. Il fatto che ciò si possa fare con mezzi che non risultano evidenti alle persone e che possa essere difficile per loro comprendere cosa sta succedendo aggrava l'impatto sulla loro vita privata. Gli ISP dovrebbero stabilire quali siano i mezzi meno invasivi disponibili per conseguire i risultati richiesti: per esempio, è possibile raggiungere l'obiettivo desiderato con il monitoraggio degli *header IP*, anziché ricorrere all'ispezione approfondita dei pacchetti di dati? Anche quando si ricorre all'ispezione approfondita dei pacchetti di dati, può essere sufficiente identificare soltanto determinati protocolli per avere le informazioni necessarie. Inoltre, può essere opportuna anche l'applicazione di clausole di salvaguardia per la protezione dei dati, tra cui la pseudo-anonimizzazione. L'esito della valutazione deve confermare che il trattamento dei dati rispetta il principio di proporzionalità.

72. *Gli effetti del trattamento (direttamente legati alle sue finalità).* Il principio di proporzionalità potrebbe non essere soddisfatto nei casi in cui gli ISP impieghino politiche di gestione del traffico che escludono l'accesso a determinati servizi senza consentire agli utenti, in cambio, un'equa condivisione dei benefici che ne risultano.

73. È importante rammentare che il principio di proporzionalità viene comunque applicato anche se sono stati soddisfatti altri requisiti giuridici, incluso il caso in cui un ISP abbia, per esempio, ottenuto il consenso dalle persone per effettuare il monitoraggio di contenuti. Ciò significa che il trattamento dei dati eseguito mediante tale monitoraggio può risultare comunque illegale se viola il principio di proporzionalità, che è fondamentale e implicito.

V.4. **Misure organizzative e di sicurezza**

74. L'articolo 4 della direttiva e-privacy impone esplicitamente agli ISP di adottare misure tecniche e organizzative per garantire i) che l'accesso ai dati personali sia consentito soltanto a personale autorizzato e per finalità lecite, ii) la protezione dei dati personali dal trattamento accidentale o illecito, nonché iii) l'attuazione di una politica di sicurezza relativamente al trattamento dei dati personali. La stessa direttiva consente, inoltre, alle autorità nazionali competenti di effettuare *audit* su queste misure.

75. Inoltre, ai sensi dell'articolo 4, paragrafi 3 e 2, della direttiva e-privacy, gli ISP sono anche tenuti a informare rispettivamente le autorità nazionali competenti in caso di violazione dei dati e le persone coinvolte qualora sussista il rischio che vi siano conseguenze negative per loro a seguito della divulgazione di tali dati.

76. Il trattamento, al fine di applicare politiche di gestione del traffico, di informazioni personali contenute nell'ambito di una comunicazione può fornire agli ISP l'accesso a dati ancora più sensibili di quelli sul traffico.

([34]) Come affermato in precedenza, la direttiva sulla protezione dei dati si applica a tutti gli aspetti riguardanti la tutela dei diritti e delle libertà fondamentali non specificamente contemplati dalla direttiva e-privacy.

77. Pertanto le politiche di sicurezza definite dagli ISP dovrebbero includere clausole di salvaguardia specifiche per garantire che le misure adottate siano adeguate rispetto ai rischi; contemporaneamente, le autorità nazionali competenti che valutano queste misure devono essere particolarmente esigenti. Infine, occorre assicurare l'attuazione di procedure di notifica efficaci per informare gli interessati le cui informazioni siano risultate compromesse e che pertanto rischiano di subire ripercussioni negative.

VI. **SUGGERIMENTI PER LE MISURE POLITICHE E LEGISLATIVE**

78. Le tecnologie di controllo basate sui dati relativi al traffico e sull'ispezione dei *payload IP*, per esempio il contenuto delle comunicazioni, potrebbero fornire notizie sull'attività degli utenti in Internet: siti Internet visitati e operazioni effettuate su tali siti, utilizzo di applicazioni P2P, file scaricati, e-mail inviate e ricevute, il nome dei loro mittenti, l'oggetto e così via. È possibile che gli ISP vogliano servirsi di queste informazioni per dare la priorità ad alcuni tipi di comunicazione, per esempio il *video on demand*, rispetto ad altri, e che vogliano utilizzarle per individuare virus o creare profili allo scopo di effettuare pubblicità comportamentale. Queste azioni pregiudicano il diritto alla riservatezza delle comunicazioni.

79. Le implicazioni per la vita privata aumentano in base alle tecnologie impiegate e alle circostanze del caso. Più l'intercettazione e l'analisi delle informazioni raccolte si spingono a fondo, maggiore è il conflitto con il principio della riservatezza delle comunicazioni. Anche le finalità per cui si effettua il monitoraggio e le clausole di salvaguardia per la protezione dei dati applicate rappresentano elementi chiave per stabilire il livello di interferenza nella vita privata e nei dati delle persone fisiche. Il blocco e il monitoraggio per la lotta al *malware*, con rigide limitazioni alla conservazione e all'utilizzo dei dati soggetti a controllo, non si possono paragonare a situazioni in cui le informazioni vengono registrate per la creazione di profili individuali a fini di pubblicità comportamentale.

80. In linea di principio, il GEPD ritiene che il quadro europeo vigente in materia di protezione dei dati e della vita privata, se correttamente interpretato, applicato e fatto rispettare, sia adatto a garantire che venga osservato il diritto alla riservatezza e soprattutto che non sia compromessa la protezione dei dati e della vita privata delle persone fisiche ([35]). Gli ISP non dovrebbero avvalersi di tali meccanismi a meno che non abbiano correttamente applicato il quadro giuridico. In particolare, gli elementi del quadro giuridico che gli ISP devono considerare e rispettare sono, tra gli altri, i seguenti:

— gli ISP possono applicare politiche di gestione del traffico ai fini della sicurezza e della prestazione del servizio, per esempio riducendo la congestione di rete, in base agli articoli 4 e 6 della direttiva e-privacy,

— per applicare politiche di gestione del traffico che comportino il trattamento dei dati sul traffico e/o sulla comunicazione con finalità diverse da quelle di cui sopra, gli ISP devono avere un'altra base giuridica specifica e possibilmente il consenso degli utenti. Per esempio, è necessario il consenso informato degli utenti per monitorare e filtrare le comunicazioni di persone fisiche al fine di limitare (o permettere) l'accesso a determinati servizi e applicazioni come il P2P o il VoIP,

— il consenso deve essere libero, esplicito e informato e manifestarsi mediante un atto affermativo. Questi requisiti evidenziano soprattutto la necessità di accrescere gli sforzi per garantire che le persone vengano correttamente informate e in modo diretto, comprensibile e specifico affinché possano valutare gli effetti delle pratiche e infine prendere una decisione informata. Considerata la complessità di queste tecnologie, fornire informazioni preliminari valide agli utenti è uno dei principali presupposti per ottenere un consenso valido. Inoltre, non devono esserci conseguenze negative (né l'addebito di costi finanziari) per gli utenti che non esprimono il loro consenso ad alcun tipo di monitoraggio,

([35]) Ciò non deve pregiudicare la necessità di apportare modifiche legislative basate su altre considerazioni, specialmente nel contesto della revisione generale del quadro giuridico europeo per la protezione dei dati, per rendere la normativa più efficace tenendo conto delle nuove tecnologie e della globalizzazione.

— il principio di proporzionalità svolge un ruolo cruciale quando gli ISP attuano politiche di gestione del traffico, a prescindere dalla base giuridica e dalla finalità del trattamento (effettuare il servizio, evitare la congestione od offrire abbonamenti mirati con o senza accesso a determinati servizi e applicazioni). Questo principio limita la capacità degli ISP di monitorare il contenuto delle comunicazioni personali trattando una quantità eccessiva di informazioni o accumulando benefici a proprio esclusivo vantaggio. Ciò che gli ISP possono fare a livello logistico dipende dal livello di invasività delle tecnologie, dai risultati richiesti (per i quali possono accumulare benefici) e dalle clausole di salvaguardia specifiche applicate in materia di protezione dei dati e della vita privata. Prima di sviluppare tecnologie di controllo, gli ISP devono effettuare una valutazione per stabilire se queste tecnologie siano conformi al principio di proporzionalità.

81. Se è vero che attualmente il quadro giuridico prevede condizioni e clausole di salvaguardia in materia, occorre verificare con particolare attenzione che gli ISP soddisfino effettivamente i requisiti giuridici, che forniscano ai consumatori le informazioni necessarie per operare scelte consapevoli e che rispettino il principio di proporzionalità. A livello nazionale, le autorità competenti per queste verifiche comprendono da una parte le autorità nazionali responsabili delle telecomunicazioni e, dall'altra, le autorità nazionali garanti della protezione dei dati. A livello di Unione europea, invece, tra gli organi competenti figura il BEREC, ma anche il GEPD può svolgere un ruolo in tale contesto.

82. Data la relativa novità rappresentata dal fatto di poter controllare molte comunicazioni in tempo reale, oltre al monitoraggio dell'attuale livello di conformità, vi sono alcuni aspetti relativi all'applicazione del quadro, affrontati nel presente parere, che richiedono un'analisi ancora più approfondita e ulteriori chiarimenti. È necessario un orientamento relativo a diversi settori che riguardi, tra gli altri:

— la determinazione delle pratiche di controllo lecite e finalizzate a garantire la fluidità del traffico che non richiedano necessariamente il consenso degli utenti, per esempio la lotta allo *spam*. Oltre all'invasività del monitoraggio effettuato, ci sono altri aspetti da considerare, come ad esempio il livello di perturbazione del traffico che si verificherebbe senza tale monitoraggio,

— la determinazione delle tecnologie di controllo impiegabili per scopi di sicurezza che non richiedano necessariamente il consenso degli utenti,

— la determinazione dei casi in cui sia necessario il consenso delle persone fisiche, in particolare di tutti gli utenti interessati, e dei parametri tecnici ammissibili al fine di garantire che la tecnica di controllo non implichi un trattamento di dati sproporzionato rispetto alle finalità da esso previste,

— inoltre, nei tre casi appena esposti, può essere necessario un orientamento sull'applicazione delle clausole di salvaguardia necessarie per la protezione dei dati (limitazione delle finalità, sicurezza e così via).

83. Poiché le competenze in questo campo sono tanto europee quanto nazionali, il GEPD ritiene che sia fondamentale condividere opinioni ed esperienze per stabilire strategie armonizzate per le questioni in esame. A tale scopo, il GEPD suggerisce di creare una piattaforma o un gruppo di esperti costituito da rappresentanti di autorità nazionali di regolamentazione, del gruppo di lavoro «articolo 29», del GEPD e del BEREC. Il primo obiettivo di questa piattaforma dovrebbe essere lo sviluppo di un orientamento, almeno sui temi summenzionati, per garantire che le strategie stabilite siano solide, armonizzate e omogenee. Il GEPD invita la Commissione a organizzare questa iniziativa.

84. Infine, sia le autorità nazionali che le rispettive omologhe europee, tra cui il BEREC e la Commissione europea, devono prestare particolare attenzione agli sviluppi del mercato in quest'ambito. Dal punto di vista della protezione dei dati e della vita privata, sarebbe estremamente problematico uno scenario in cui gli ISP attuino abitualmente politiche di gestione del traffico offrendo abbonamenti che comportano il filtraggio dell'accesso ai contenuti e alle applicazioni. Se ciò dovesse accadere, si dovrebbero adottare misure legislative per affrontare tale situazione.

VII. **CONCLUSIONI**

85. Il fatto che gli ISP facciano sempre più affidamento sulle tecnologie di monitoraggio e di controllo influisce sulla neutralità di Internet e sulla riservatezza delle comunicazioni, sollevando gravi problemi relativi alla protezione dei dati personali e della vita privata degli utenti.

86. Anche se la comunicazione della Commissione sull'apertura e la neutralità della rete Internet in Europa accenna brevemente a questi problemi, il GEPD ritiene che si debba fare di più per determinare una politica soddisfacente per il futuro e nel presente parere ha pertanto contribuito al dibattito politico in corso sulla neutralità della rete, soprattutto per quanto riguarda gli aspetti legati alla protezione dei dati e della vita privata.

87. Il GEPD ritiene, inoltre, necessario che le autorità nazionali e il BEREC monitorino la situazione del mercato, in modo da tracciare un quadro esauriente per stabilire se il mercato si stia evolvendo verso un controllo massiccio e in tempo reale delle comunicazioni senza trascurare le questioni attinenti all'osservanza del quadro giuridico.

88. Il monitoraggio del mercato deve includere un'analisi approfondita degli effetti delle nuove pratiche sulla protezione dei dati e della vita privata nella rete Internet. Il presente parere menziona alcuni settori che trarrebbero vantaggio da un chiarimento. Se le agenzie europee e organi come il BEREC, il gruppo di lavoro «articolo 29» e il GEPD possono trovarsi in una buona posizione per chiarire le condizioni di applicazione del quadro, lo stesso GEPD ritiene che la Commissione abbia il dovere di coordinare e guidare il dibattito e pertanto la esorta a prendere l'iniziativa coinvolgendo tutte le parti interessate in una piattaforma o in un gruppo di lavoro che abbia questo obiettivo. Fra i temi che devono essere ulteriormente esaminati, sarà necessario affrontare i punti seguenti:

— determinare le pratiche di controllo che sono lecite per garantire la fluidità del traffico e che possono essere adottate a scopi di sicurezza,

— determinare in quali casi il monitoraggio richieda il consenso delle persone fisiche, e in particolare di tutti gli utenti interessati, e quali parametri tecnici siano ammessi per garantire che la tecnologia di ispezione non implichi un trattamento di dati sproporzionato rispetto alle finalità previste,

— nei casi summenzionati può rendersi necessario un orientamento riguardante l'applicazione delle clausole di salvaguardia necessarie in materia di protezione dei dati (limitazione delle finalità, sicurezza e così via).

89. In base a queste conclusioni, possono risultare necessari provvedimenti legislativi supplementari. In tal caso, la Commissione dovrebbe proporre misure di carattere politico volte a consolidare il quadro giuridico e a garantire la certezza del diritto. Le nuove misure dovrebbero fare chiarezza sulle conseguenze pratiche del principio di neutralità della rete, poiché ciò è già stato fatto in alcuni Stati membri, e assicurare che gli utenti abbiano effettivamente la possibilità di scegliere, soprattutto obbligando gli ISP a offrire connessioni non monitorate.

Fatto a Bruxelles, il 7 ottobre 2011

Peter HUSTINX

Garante europeo della protezione dei dati