ISSN 1725-2466

Gazzetta ufficiale dell'Unione europea

C 280

Edizione in lingua italiana

53° anno

16 ottobre 2010

Comunicazioni e informazioni

IT

Prezzo: 3 EUR

[1] Testo rilevante ai fini del SEE, eccetto per i prodotti dell'allegato I del trattato

(segue)

IT

[1] Testo rilevante ai fini del SEE, eccetto per i prodotti dell'allegato I del trattato
[2] Testo rilevante ai fini del SEE

(segue in 3ª pagina di copertina)

I

(Risoluzioni, raccomandazioni e pareri)

PARERI

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del Garante europeo della protezione dei dati sulla promozione della fiducia nella società dell'informazione tramite l'incentivazione della protezione dei dati e della vita privata

(2010/C 280/01)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

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

vista la Carta dei diritti fondamentali dell'Unione europea, in particolare gli articoli 7 e 8,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ([1]),

vista la 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 ([2]),

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 ([3]), in particolare l'articolo 41,

HA ADOTTATO IL SEGUENTE PARERE:

I. **INTRODUZIONE**

1. Le tecnologie dell'informazione e della comunicazione (TIC) offrono straordinarie capacità in quasi ogni aspetto delle nostre vite: nel nostro modo di lavorare, giocare, socializzare e istruirci. Sono essenziali per l'odierna economia dell'informazione e per la società in generale.

2. L'Unione europea è una forza globale nelle TIC avanzate ed è determinata a rimanere tale. Per rispondere a questa sfida, si prevede che la Commissione europea adotterà tra breve una nuova Agenda europea del digitale, che la commissaria Kroes ha confermato quale sua priorità ([4]).

3. Il GEPD riconosce i vantaggi che derivano dalle TIC e concorda sul fatto che l'UE dovrebbe adoperarsi al massimo per incentivarne lo sviluppo e l'adozione diffusa. Egli sottoscrive, inoltre, pienamente i pareri dei commissari Kroes e Reding secondo cui gli individui dovrebbero essere al centro di questo nuovo ambiente ([5]). Gli individui dovrebbero poter contare sulla capacità delle TIC di mantenere le loro informazioni al sicuro e di controllarne l'uso e dovrebbero avere la garanzia che i loro diritti alla riservatezza e alla tutela dei dati saranno rispettati nello spazio digitale. Il rispetto di questi diritti è essenziale per generare la fiducia nei consumatori e tale fiducia è fondamentale se si vuole che i cittadini ricorrano a nuovi servizi ([6]).

([1]) GU L 281 del 23.11.1995, pag. 31.
([2]) GU L 201 del 31.7.2002, pag. 37.
([3]) GU L 8 del 12.1.2001, pag. 1.

([4]) Risposte al questionario del Parlamento europeo per la commissaria Neelie Kroes nell'ambito dell'audizione del PE che ha preceduto la nomina della commissaria.
([5]) Risposte al questionario del Parlamento europeo per la commissaria Neelie Kroes nell'ambito dell'audizione del PE che ha preceduto la nomina della commissaria; discorso della commissaria Viviane Reding su «A European Digital Agenda for the New Digital Consumer» (Un'Agenda europea del digitale per il nuovo consumatore digitale), tenuto presso il Forum multilaterale del BEUC su «Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives» (Vita privata del consumatore e marketing on-line: tendenze del mercato e prospettive politiche), Bruxelles 12 novembre 2009.
([6]) Cfr., ad esempio, la relazione RISEPTIS, «Trust in the Information Society» (Fiducia nella società dell'informazione), una relazione del consiglio consultivo, RISEPTIS (ricerca e innovazione per la sicurezza, la vita privata e l'affidabilità nella società dell'informazione). Disponibile all'indirizzo (http://www.think-trust.eu/general/news-events/riseptis-report.html). Cfr. inoltre: J. B Horrigan, Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, *OBI Working Paper Series No. 1*.

4. L'UE ha un solido quadro giuridico di protezione dei dati/vita privata, i cui principi rimangono completamente validi nell'era digitale. Tuttavia, ciò non è sufficiente. In molti casi, le TIC sollevano nuove preoccupazioni di cui non si tiene conto nel quadro attuale. Pertanto sono necessarie alcune azioni per garantire che i diritti individuali, sanciti nella legislazione dell'UE, continuino ad assicurare una protezione efficace in questo nuovo ambiente.

5. Il presente parere tratta delle misure che potrebbero essere promosse o intraprese dall'Unione europea al fine di garantire la protezione della vita privata e dei dati degli individui in un mondo globalizzato, che rimarrà guidato dalla tecnologia. Esso discute gli strumenti legislativi e non legislativi.

6. Dopo aver fornito una descrizione generale delle TIC quale nuovo sviluppo che crea opportunità ma anche rischi, il parere esamina la necessità di integrare, a livello pratico, la tutela dei dati e la riservatezza fin dall'inizio delle nuove tecnologie dell'informazione e della comunicazione (indicato come principio della «Privacy by Design», ovvero tutela della vita privata fin dalla progettazione). Per imporre la conformità con questo principio, il parere tratta della necessità di tenere conto del principio della tutela della vita privata fin dalla progettazione nel quadro giuridico di protezione dei dati in almeno due modi diversi. In primo luogo, integrandolo quale principio generale e vincolante e, in secondo luogo, incorporandolo in particolari ambiti delle TIC, che presentano rischi specifici per la protezione dei dati/vita privata, i quali possono essere attenuati attraverso un'adeguata architettura e progettazione tecnica. Tali ambiti sono l'identificazione a radiofrequenza (RFID), le applicazioni di social network e i browser. Per concludere, il parere indica suggerimenti relativi ad altri strumenti e principi destinati a proteggere la vita privata e la tutela dei dati degli individui nel settore delle TIC.

7. Nel trattare di quanto sopra, il parere approfondisce alcuni punti espressi dal gruppo dell'articolo 29 nel suo contributo alla consultazione pubblica sul futuro della vita privata ([1]). Inoltre, si basa su pareri precedenti del GEPD, come il parere del 25 luglio 2007 sull'attuazione della direttiva sulla protezione dei dati, sul parere del 20 dicembre 2007 sulla RFID e sui suoi due pareri sulla direttiva e-privacy ([2]).

II. LE TIC OFFRONO NUOVE OPPORTUNITÀ MA PRESENTANO ANCHE NUOVI RISCHI

8. Le TIC sono state paragonate ad altre importanti invenzioni del passato, come l'elettricità. Mentre può essere troppo presto per valutare il loro effetto storico reale, il collegamento tra le TIC e lo sviluppo economico nei paesi sviluppati è evidente. Le TIC hanno creato occupazione, benefici economici e hanno contribuito al benessere generale. L'effetto delle TIC va oltre il lato puramente economico, perché hanno svolto un ruolo importante nell'incentivare l'innovazione e la creatività.

9. Inoltre, le TIC hanno trasformato il modo in cui le persone lavorano, socializzano e interagiscono. Ad esempio, le persone utilizzano sempre più le TIC per le interazioni sociali ed economiche. Gli individui possono usare una vasta gamma di nuove applicazioni TIC, quali sanità elettronica, trasporti elettronici e amministrazione elettronica, nonché sistemi interattivi innovativi per l'intrattenimento e l'apprendimento.

10. Alla luce di tali benefici, le istituzioni europee hanno espresso tutte il loro impegno a sostenere le TIC quale strumento necessario a migliorare la competitività dell'industria europea e ad accelerare la ripresa economica dell'Europa. In effetti, nell'agosto 2009 la Commissione ha adottato la Relazione sulla competitività digitale in Europa ([3]) e ha avviato una consultazione pubblica sulle strategie future adeguate per incentivare le TIC. Il 7 dicembre 2009, il Consiglio ha proposto un contributo a questa consultazione, dal titolo «Post i2010 Strategy — Toward an open, green and competitive knowledge society» (Strategia Post i2010 — Verso una società dell'informazione aperta, verde e competitiva) ([4]). Il Parlamento

([1]) Parere 168 del gruppo dell'articolo 29 sul futuro della vita privata, contributo congiunto alla consultazione della Commissione europea sul quadro legale per il diritto fondamentale alla protezione dei dati personali, adottato il 1º dicembre 2009.

([2]) Parere del 25 luglio 2007 del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati, GU C 255 del 27.10.2007, pag. 1; parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni — L'identificazione a radiofrequenza (RFID) in Europa: verso un quadro politico, documento [COM(2007) 96], GU C 101 del 23.4.2008, pag. 1; parere del 10 aprile 2008 del Garante europeo della protezione dei dati sulla proposta di direttiva del Parlamento europeo e del Consiglio recante modifica, tra l'altro, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), GU C 181 del 18.7.2008, pag. 1; secondo parere del 9 gennaio 2009 del Garante europeo della protezione dei dati sulla revisione della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

([3]) Relazione sulla competitività digitale in Europa — Principali risultati della strategia i2010 nel periodo 2005-2009, [SEC(2009) 1060].

([4]) Conclusioni del Consiglio «Post i-2010 Strategy- Towards and Open, Green and Competitive Knowledge Society» (Verso una società dell'informazione aperta, verde e competitiva) (17107/09), adottate il 18.12.2009.

europeo ha recentemente adottato una relazione destinata a fornire orientamenti alla Commissione nella definizione di un'agenda digitale ([1]).

11. Con le opportunità e i benefici che accompagnano lo sviluppo delle TIC arrivano nuovi rischi, soprattutto per la vita privata e la protezione dei dati personali degli individui. Le TIC conducono spesso a una proliferazione (abbastanza spesso in modi nascosti agli individui) della quantità di informazioni raccolte, smistate, filtrate, trasferite oppure conservate e i rischi per tali dati si moltiplicano di conseguenza.

12. Ad esempio, i chip RFID stanno sostituendo i codici a barre su alcuni generi di consumo. Migliorando il flusso delle informazioni nella catena di rifornimento (e riducendo in tal modo l'esigenza di riserve «di sicurezza», fornendo previsioni più esatte, ecc.) si prevede che il nuovo sistema fornirà vantaggi sia alle attività commerciali che ai consumatori. Tuttavia, allo stesso tempo, ciò solleva la possibilità preoccupante di essere rintracciati, per diversi scopi e da entità differenti, attraverso proprietà personali etichettate.

13. Un altro esempio è il cosiddetto «cloud computing», essenzialmente la fornitura di servizi di applicazioni di consumo e non, ospitati su Internet. Tali servizi vanno da librerie fotografiche, calendari, webmail e banche dati di clienti a servizi più complessi legati al commercio. I benefici per le aziende e gli individui sono evidenti: riduzione dei costi (i costi sono incrementali), assenza di sedi (facile accesso alle informazioni ovunque nel mondo), automazione (nessuna necessità di risorse IT dedicate e di mantenere il software aggiornato) ecc. Contemporaneamente, esistono rischi reali di violazione della sicurezza e di pirateria informatica. Vi è inoltre la preoccupazione di perdere l'accesso e il controllo sui propri dati.

14. È stato dimostrato che benefici e rischi coesistono anche in altri ambiti che utilizzano applicazioni TIC. Si consideri la sanità elettronica, che può aumentare l'efficacia, ridurre i costi, aumentare l'accessibilità e generalmente migliorare la qualità dei servizi sanitari. Tuttavia, la sanità elettronica solleva spesso la questione della legittimità degli usi secondari delle sue informazioni, che richiede un'attenta analisi degli scopi di qualsiasi possibile utilizzo secondario ([2]). Inoltre, con l'utilizzo più diffuso delle cartelle cliniche elettroniche, i sistemi stessi sono stati bersagliati da scandali che hanno rivelato molti casi di intrusione in tali cartelle.

15. Nel complesso, è probabile che persista un certo grado di rischio residuo, anche dopo aver fatto le valutazioni corrette e dopo aver applicato le misure necessarie. Una situazione senza rischi sarebbe irrealistica. Tuttavia, come discusso ulteriormente di seguito, le misure possono e devono essere attuate per ridurre tale rischio a livelli adeguati.

III. LA TUTELA DELLA VITA PRIVATA SIN DALLA PROGETTAZIONE QUALE STRUMENTO PRINCIPALE DI CREAZIONE DI FIDUCIA NELLE TIC PRESSO I SINGOLI INDIVIDUI

16. I potenziali benefici delle TIC possono essere sfruttati in pratica soltanto se sono in grado di generare fiducia, in altri termini, se possono assicurare la disponibilità degli utenti a dipendere dalle TIC a causa delle loro caratteristiche e vantaggi. Tale fiducia si produrrà soltanto se le TIC saranno affidabili, sicure, sotto il controllo degli individui e se verrà garantita la protezione dei dati e della vita privata.

17. I rischi e gli errori diffusi come quelli illustrati sopra, specialmente quando comportano l'uso improprio o le violazioni dei dati personali che espongono la vita privata degli individui, hanno forti probabilità di mettere in pericolo la fiducia degli utenti nella società dell'informazione. Ciò potrebbe compromettere seriamente lo sviluppo delle TIC e i benefici che potrebbe portare.

18. Tuttavia, la soluzione a questi rischi per la vita privata e la protezione dei dati non può essere di eliminare, escludere o rifiutare di utilizzare o promuovere le TIC. Ciò non sarebbe né fattibile né realistico, impedirebbe agli individui di godere dei benefici delle TIC e limiterebbe seriamente i vantaggi generali da ottenere.

19. Il GEPD ritiene che una soluzione più positiva consista nel progettare e sviluppare le TIC in modo da rispettare la vita privata e la protezione dei dati. È quindi fondamentale che la vita privata e la protezione dei dati siano incluse all'interno dell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla loro ultima distribuzione, all'utilizzo e all'eliminazione finale. Ciò viene indicato generalmente come principio della «privacy by design» (PbD, tutela della vita privata sin dalla progettazione) e viene trattato ulteriormente di seguito.

20. La PbD può comprendere azioni differenti, secondo il caso particolare o l'applicazione. Ad esempio, può richiedere in alcuni casi l'eliminazione/la riduzione dei dati personali o il divieto dell'elaborazione inutile e/o indesiderata. In altri casi, la PbD può comportare l'offerta di strumenti destinati ad aumentare il controllo degli individui sui loro dati personali. Queste misure dovrebbero essere considerate quando vengono definiti standard e/o migliori prassi. Esse possono essere anche integrate nell'architettura dei

([1]) Relazione sulla Definizione di una nuova agenda digitale per l'Europa: da i2010 a digital.eu [2009/2225 (INI)], adottata il 18.3.2010.

([2]) Ad esempio, non è possibile vendere o utilizzare le informazioni sanitarie raccolte a scopo terapeutico per selezionare luoghi per cliniche satelliti, per istituire centri chirurgici ambulatoriali e, diversamente, progettare attività future con implicazioni finanziarie richiederebbe un esame attento.

sistemi di informazione e comunicazione, o nelle organizzazioni strutturali delle entità che elaborano i dati personali.

III.1. **Principio della tutela della vita privata sin dalla progettazione applicabile in diversi ambienti TIC e suoi effetti**

21. L'esigenza del principio della tutela della vita privata fin dalla progettazione può essere individuata in molti ambienti TIC diversi. Ad esempio, il settore della sanità si basa sempre più sulle infrastrutture TIC, che richiedono spesso l'archiviazione centralizzata di informazioni correlate alla salute dei pazienti. L'applicazione del principio di PbD nel settore sanitario richiederebbe la valutazione dell'idoneità di diverse misure quali la possibilità di ridurre al minimo i dati memorizzati a livello centrale o di limitarli a un indice, tramite strumenti di crittografia, l'assegnazione di diritti di accesso limitatamente alla «necessità di conoscenza», l'anonimizzazione dei dati una volta che non siano più necessari, ecc.

22. Analogamente, i sistemi di trasporto sono sempre più forniti di serie di applicazioni TIC avanzate che interagiscono con il veicolo e il suo ambiente per diversi scopi e funzioni. Ad esempio, le automobili sono sempre più dotate di nuove funzionalità TIC (GPS, GSM, rete di sensori, ecc.) che forniscono non solo la loro posizione ma anche le loro condizioni tecniche in tempo reale. Queste informazioni potrebbero essere utilizzate, ad esempio, per sostituire l'attuale sistema di tassazione degli autoveicoli con un pedaggio legato all'utente. L'applicazione di PbD alla struttura dell'architettura di tali sistemi dovrebbe sostenere l'elaborazione e il trasferimento progressivo del minor numero possibile di dati personali ([1]). In linea con questo principio, sarebbero preferibili le architetture decentralizzate o semi-decentralizzate, che limitano la rivelazione dei dati sull'ubicazione, rispetto a quelle decentralizzate.

23. Gli esempi riportati sopra mostrano che quando le tecnologie dell'informazione e della comunicazione sono sviluppate secondo il principio della PbD, i rischi per la vita privata e la protezione dei dati possono essere ridotti in maniera significativa.

([1]) Cfr. il parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione sul piano d'azione per la diffusione di sistemi di trasporto intelligenti in Europa e sulla relativa proposta di direttiva del Parlamento europeo e del Consiglio che istituisce il quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto, disponibile all'indirizzo: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

III.2. **Diffusione insufficiente delle TIC che applicano la tutela della vita privata fin dalla progettazione**

24. Una domanda importante è se gli operatori economici, i produttori/fornitori di TIC e i responsabili del trattamento di dati sono interessati a diffondere e ad attuare il principio della PbD nelle TIC. In questo contesto, è importante valutare, inoltre, la domanda degli utenti di PbD.

25. Nel 2007 la Commissione ha pubblicato una comunicazione in cui invitava le aziende a utilizzare il loro potere di innovazione per creare e attuare le tecnologie di rafforzamento della tutela della vita privata quale modo per migliorare la protezione della vita privata e dei dati personali fin dall'inizio del ciclo di sviluppo ([2]).

26. Finora, tuttavia, le prove disponibili indicano che né i fornitori di TIC né i responsabili del trattamento dei dati (nel settore privato o pubblico) sono riusciti ad attuare o a diffondere in maniera costante la PbD. Sono state addotte motivazioni diverse, tra cui la mancanza di incentivi economici o di supporto istituzionale, una domanda insufficiente e altro ancora ([3]).

27. Allo stesso tempo, la domanda di PbD da parte degli utenti è stata piuttosto scarsa. Gli utenti di prodotti e servizi TIC possono supporre giustamente che la loro vita privata e i loro dati personali sono protetti de facto, quando in molti casi, non lo sono. In alcuni casi, non sono semplicemente nella posizione di adottare le misure di sicurezza necessarie a proteggere i loro dati personali o quelli di altri. In molti casi questo accade perché manca loro la conoscenza completa o persino parziale dei rischi. Ad esempio, in linea generale i giovani non considerano i rischi per la vita privata connessi alla visualizzazione di informazioni personali sulle reti sociali e spesso ignorano le impostazioni della privacy. Altri utenti ancora sono consapevoli dei rischi ma potrebbero non avere l'esperienza tecnica necessaria per mettere in atto tecnologie di protezione, come quelle che proteggono il loro collegamento a Internet o le modifiche delle impostazioni del browser per ridurre al minimo la creazione di profili basata sul controllo delle loro attività di navigazione in Internet.

28. Tuttavia, i rischi per la protezione della vita privata e dei dati sono molto reali. Se la protezione della vita privata e dei dati non vengono presi in considerazione fin dall'inizio, è spesso troppo tardi ed economicamente troppo

([2]) Comunicazione del 2.5.2007, COM(2007) 228 definitivo, comunicazione della Commissione al Parlamento europeo e al Consiglio sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET).

([3]) Studio sui benefici economici delle tecnologie di rafforzamento della riservatezza (PET), JLS/2008/D4/036.

complicato riparare i sistemi e troppo tardi per riparare i danni già arrecati. Il sempre maggior numero di violazioni dei dati negli ultimi anni illustra perfettamente questo problema e rinforza l'esigenza della tutela della vita privata sin dalla progettazione.

29. Quanto detto sopra suggerisce chiaramente che i produttori e i fornitori di tecnologie TIC destinate a elaborare i dati personali dovrebbero avere, insieme ai responsabili del trattamento dei dati, la responsabilità di progettarli con misure di protezione dei dati e di tutela della vita privata integrate. In molti casi ciò significherebbe che dovrebbero essere progettate con impostazioni predefinite della vita privata.

30. In questo contesto, occorre considerare quali azioni dovrebbero essere intraprese dai responsabili politici per promuovere la PbD nello sviluppo delle TIC. Una prima domanda è se il quadro legale esistente di protezione dei dati contenga disposizioni adeguate per garantire l'attuazione del principio della PbD da parte sia dei responsabili del trattamento di dati che dei produttori/sviluppatori. Una seconda domanda è che cosa dovrebbe essere fatto nel contesto dell'agenda digitale europea per assicurare che il settore delle TIC generi la fiducia dei consumatori.

IV. **INTEGRAZIONE DEL PRINCIPIO DI TUTELA DELLA VITA PRIVATA SIN DALLA PROGETTAZIONE NELLE LEGGI E NELLE POLITICHE DELL'UE**

IV.1. **L'attuale quadro legale di protezione dei dati e della vita privata**

31. L'UE dispone di un solido quadro di protezione dei dati e della vita privata sancito nella direttiva 95/46/CE [1], nella direttiva 2002/58/CE [2] e nella giurisprudenza della Corte europea dei diritti dell'uomo [3] e della Corte di giustizia.

32. La direttiva sulla protezione dei dati personali si applica a «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali» (raccolta, memorizzazione, comunicazione, ecc.). Essa impone la conformità con alcuni principi e obblighi su chi elabora i dati personali («responsabili del trattamento di dati»). Dispone diritti individuali, quali il diritto di accedere a informazioni personali. La direttiva e-privacy si occupa specificamente della protezione della vita privata nel settore delle comunicazioni elettroniche [4].

33. L'attuale direttiva sulla protezione dei dati non contiene un requisito esplicito di PbD. Tuttavia, comprende disposizioni che indirettamente, in situazioni diverse, possono richiedere effettivamente l'attuazione del principio di PbD. In particolare, l'articolo 17 richiede che il responsabile del trattamento attui misure tecniche ed organizzative appropriate al fine di impedire il trattamento illecito dei dati personali [5]. La tutela della vita privata fin dalla progettazione viene pertanto affrontata in maniera molto generica. Inoltre, le disposizioni della direttiva sono rivolte principalmente ai responsabili del trattamento dei dati e alla loro attività di trattamento dei dati personali. Non richiedono esplicitamente che le tecnologie di informazione e comunicazione siano conformi per quanto riguarda la protezione della vita privata e dei dati, il che richiede anche di proporre ai progettisti e ai produttori di TIC di includere le attività svolte in fase di normalizzazione.

34. La direttiva e-privacy è più esplicita. L'articolo 14.3 stabilisce che «All'occorrenza, possono essere adottate misure dirette a garantire che le apparecchiature terminali siano costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali in conformità della direttiva 1999/5/CE e della decisione 87/95/CEE del Consiglio, del 22 dicembre 1986, relativa alla normalizzazione nel settore delle tecnologie dell'informazione delle telecomunicazioni)». Tuttavia, questa disposizione non è mai stata utilizzata [6].

35. Sebbene le disposizioni di cui sopra delle due direttive siano utili ai fini della promozione della tutela della vita privata fin dalla progettazione, in pratica non sono state sufficienti nell'assicurare che la vita privata fosse integrata nelle TIC.

36. Come conseguenza della situazione di cui sopra, la legge non richiede in modo sufficientemente preciso che le TIC siano progettate in conformità con il principio della tutela

(1) Direttiva 95/46/CE del Parlamento europeo e del Consiglio (nel prosieguo: direttiva sulla protezione dei dati).

(2) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio (nel prosieguo: direttiva e-privacy).

(3) Interpretazione degli elementi e delle condizioni principali stabiliti nell'articolo 8 della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) adottata a Roma il 4 novembre 1950; applicazione in diversi ambiti.

(4) Il trattato di Lisbona ha rafforzato tale protezione riconoscendo il rispetto della vita privata e della protezione dei dati personali quali diritti fondamentali separati nell'articolo 7 e 8 della Carta europea dei diritti fondamentali. Tale Carta è diventata vincolante quando è entrato in vigore il trattato di Lisbona.

(5) L'articolo 17 recita: «Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali.» Il considerando 46 lo integra affermando «considerando che la tutela dei diritti e delle libertà delle persone interessate relativamente al trattamento di dati personali richiede l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento, in particolare per garantirne la sicurezza ed impedire in tal modo qualsiasi trattamento non autorizzato».

(6) La Commissione ha annunciato dei piani per aggiornare la direttiva 1999/5/CE verso la fine del 2010.

della vita privata sin dalla progettazione. Inoltre, le autorità incaricate della protezione dei dati non hanno poteri sufficienti per assicurare che la PbD sia integrata. Ciò provoca l'inefficacia. Ad esempio, le autorità incaricate della protezione dei dati possono essere in grado di applicare sanzioni per la mancata risposta alle richieste di accesso fatte dagli individui e avranno le competenze per richiedere l'attuazione di alcune misure destinate ad evitare l'elaborazione illegale dei dati. Tuttavia non è sempre sufficientemente chiaro se i loro poteri si estendano a richiedere che un sistema sia progettato in modo da facilitare i diritti di protezione dei dati degli individui ([1]). Ad esempio, in base alle disposizioni legali attuali non è chiaro se si potrebbe richiedere che l'architettura di un sistema d'informazione sia progettata in modo da agevolare la risposta delle società alle richieste di accesso fatte dagli individui, in modo che tali richieste possano essere gestite automaticamente e più rapidamente. Inoltre, tentativi successivi di alterare la tecnologia una volta sviluppata o installata possono produrre un insieme di soluzioni che non funzionano completamente, oltre ad essere economicamente onerose.

37. Secondo il parere del GEPD, condiviso dal gruppo dell'articolo 29 ([2]), l'attuale quadro legale lascia spazio a un sostegno più esplicito del principio della PbD.

IV.2. **Integrazione della tutela della vita privata sin dalla progettazione a diversi livelli**

38. Alla luce di quanto sopra, il GEPD suggerisce alla Commissione di seguire quattro linee di condotta:

a) proporre di includere una disposizione generale sulla PbD nel quadro giuridico della protezione dei dati;

b) elaborare questa disposizione generale in disposizioni specifiche, quando vengono proposti strumenti giuridici specifici in diversi settori. Queste disposizioni specifiche hanno già potuto essere incluse in strumenti giuridici; in base all'articolo 17 della direttiva sulla protezione dei dati (e di altre leggi esistenti);

c) includere la PbD quale principio guida nell'Agenda europea del digitale;

d) introdurre la PbD quale principio in altre iniziative della UE (principalmente non legislative).

Una disposizione generale sulla tutela della vita privata sin dalla progettazione

39. Il GEPD propone di includere inequivocabilmente ed esplicitamente il principio della tutela della vita privata sin dalla progettazione nel quadro normativo esistente sulla protezione dei dati. Ciò renderebbe il principio della PbD più solido, più esplicito e ne imporrà l'attuazione efficace, oltre a dare maggiore legittimità alle autorità incaricate di farlo rispettare per richiedere la sua applicazione de facto nella pratica. Questo è particolarmente necessario alla luce dei fatti descritti sopra, non solo l'importanza del principio in sé quale strumento per promuovere la fiducia, ma anche come incentivo alle parti interessate per attuare la PbD e aumentare le garanzie indicate nel quadro giuridico attuale.

40. Questa proposta si basa sulla raccomandazione del gruppo dell'articolo 29 di introdurre il principio di «privacy by design» quale principio generale nel quadro giuridico della protezione dei dati, in particolare, nella direttiva sulla protezione dei dati. Secondo il gruppo dell'articolo 29: «This principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems. Providers of such systems or services as well as controllers should demonstrate that they have taken all measures required to comply with these requirements» (Questo principio dovrebbe essere vincolante per i progettisti e i produttori di tecnologia nonché per i responsabili del trattamento dei dati che devono decidere in merito all'acquisizione e all'uso delle TIC. Essi dovrebbero essere obbligati a tenere in considerazione la protezione tecnologica dei dati già nella fase di progettazione delle procedure e dei sistemi di informazione e tecnologici. I fornitori di tali sistemi o servizi e i responsabili del trattamento dovrebbero dimostrare di aver adottato tutte le misure necessarie a soddisfare questi requisiti).

41. Il GEPD accoglie inoltre favorevolmente l'approvazione da parte del commissario Viviane Reding del principio della tutela della vita privata sin dalla progettazione fatta nell'ambito dell'annuncio della revisione della direttiva sulla protezione dei dati ([3]).

42. Ciò porta al contenuto di tale regolamento. Per prima cosa, e più importante, un principio generale di tutela della vita privata sin dalla progettazione dovrebbe essere tecnologicamente neutro. Il principio non dovrebbe mirare a regolamentare la tecnologia, ovvero non dovrebbe

([1]) Cfr. la relazione dell'ufficio del commissario all'informazione del Regno Unito dal titolo: «Privacy by Design», pubblicata nel novembre 2008.

([2]) Parere 168 del gruppo dell'articolo 29 sul futuro della vita privata, contributo congiunto alla consultazione della Commissione europea sul quadro legale per il diritto fondamentale alla protezione dei dati personali, adottato il 1º dicembre 2009.

([3]) «Privacy by design is a principle that is in the interest of both citizens and businesses. Privacy by design will lead to better protection for individuals, as well as to trust and confidence in new services and products, that will in turn have a positive impact on the economy. There are some encouraging examples but much more needs to be done.» (La tutela della vita privata fin dalla progettazione è un principio che è nell'interesse sia dei cittadini che delle imprese. La tutela della vita privata fin dalla progettazione porterà a una migliore protezione degli individui, nonché alla fiducia e all'affidamento nei nuovi servizi e prodotti, che avranno a loro volta un effetto positivo sull'economia. Vi sono esempi incoraggianti, ma resta ancora molto da fare.) Relazione di base alla giornata sulla protezione dei dati, 28 gennaio 2010, Parlamento europeo, Bruxelles.

prescrivere soluzioni tecniche specifiche, ma dovrebbe invece stabilire che i principi esistenti di protezione della vita privata e dei dati siano integrati in sistemi e soluzioni di informazione e comunicazione. Ciò consentirebbe alle parti interessate, ai produttori, ai responsabili del trattamento dei dati e alle autorità di vigilanza di interpretare il significato del principio in ogni caso specifico. In secondo luogo, la conformità con il principio dovrebbe essere obbligatoria in diverse fasi, dalla creazione di standard e la progettazione dell'architettura alla loro attuazione da parte del responsabile del trattamento dei dati.

Disposizioni in strumenti giuridici specifici

43. Gli strumenti legislativi attuali e futuri devono integrare il principio della PbD in base all'attuale quadro giuridico e, dopo l'adozione della disposizione generale proposta sopra, in base all'ultima disposizione. Ad esempio, secondo le attuali iniziative relative ai sistemi di trasporto intelligenti la Commissione avrà una responsabilità iniziale specifica nella definizione di misure, iniziative di normalizzazione, procedure e migliori pratiche. Nell'assolvimento di queste mansioni, il principio guida dovrebbe essere quello della PbD.

44. Il GEPD osserva, inoltre, che il principio della tutela della vita privata sin dalla progettazione ha un'importanza specifica anche nell'ambito della libertà, della sicurezza e della giustizia, in particolare rispetto agli obiettivi della strategia di gestione delle informazioni, come previsto nel programma di Stoccolma ([1]). Nel suo parere relativo al programma di Stoccolma il GEPD ha sottolineato il fatto che l'architettura per lo scambio di informazioni dovrebbe essere basata sulla «privacy by design» ([2]): «Ciò significa più concretamente che i sistemi di informazione progettati per finalità di sicurezza pubblica dovrebbero sempre essere costruiti conformemente al principio della "tutela della vita privata fin alla progettazione"».

45. Il parere del gruppo dell'articolo 29 sul futuro della vita privata ([3]) insiste in termini ancora più precisi sul fatto che nel campo della libertà, della sicurezza e della giustizia, dove le autorità pubbliche sono gli attori principali e dove le misure che aumentano la sorveglianza influiscono direttamente sui diritti fondamentali alla protezione della vita privata e dei dati, i requisiti della tutela della vita privata sin dalla progettazione dovrebbero essere resi obbligatori. Introducendo questi requisiti nei sistemi d'informazione, i governi stimolerebbero inoltre la tutela della vita privata sin dalla progettazione nella loro funzione di clienti di riferimento.

La tutela della vita privata sin dalla progettazione quale principio guida dell'Agenda europea del digitale

46. Le tecnologie dell'informazione e della comunicazione sono sempre più complesse e comportano maggiori rischi per la protezione della vita privata e dei dati. In generale, le informazioni digitalizzate, cui è più facile avere accesso e che è più agevole copiare e trasmettere, sono esposte a rischi molto più elevati delle informazioni scritte. Avanzando verso le reti di oggetti interconnessi, i rischi aumenteranno. Maggiori sono i rischi per la protezione della vita privata/dei dati, più elevata sarà la domanda di una maggiore protezione dei dati/tutela della vita privata. Di conseguenza, le giustificazioni alla necessità di attuare la PbD sono più impellenti nel settore delle TIC. Inoltre, come discusso sopra, la fiducia degli individui nelle TIC è fondamentale perché i cittadini scelgano questi nuovi servizi e la vita privata e la protezione dei dati sono elementi fondamentali di tale fiducia.

47. Quanto esposto sopra sottolinea il fatto che una strategia per lo sviluppo delle TIC deve confermare la necessità che siano progettate con un elemento intrinseco di protezione della vita privata e dei dati, ovvero prendendo in considerazione il principio di tutela della vita privata sin dalla progettazione.

48. Di conseguenza, l'Agenda europea del digitale dovrebbe approvare esplicitamente il principio di tutela della vita privata sin dalla progettazione come elemento necessario per assicurare la fiducia dei cittadini nelle TIC e nei servizi on-line. Dovrebbe riconoscere che la vita privata e la fiducia vanno di pari passo e che la tutela della vita privata sin dalla progettazione deve essere un fattore guida nello sviluppo di un settore delle TIC affidabile.

La tutela della vita privata sin dalla progettazione quale principio in altre iniziative dell'UE

49. La Commissione dovrebbe avere come principio guida la tutela della vita privata sin dalla progettazione nell'attuazione di politiche, attività e iniziative in specifici settori delle TIC, tra cui la sanità elettronica, gli appalti elettronici, la previdenza sociale elettronica, l'e-learning ecc. Molte di queste iniziative saranno punti di azione nell'Agenda europea del digitale.

50. Ciò significa, ad esempio, che le iniziative per assicurare che le applicazioni di amministrazione siano più efficienti e moderne in modo che gli individui possano interagire con le amministrazioni dovrebbero includere la necessità che siano progettate e operate in conformità con il principio della tutela della vita privata sin dalla progettazione. Lo stesso discorso vale per le politiche e le attività della Commissione che provvedono a un Internet più veloce, ai contenuti digitali, o alla promozione globale delle comunicazioni fisse e senza fili e della trasmissione dei dati.

([1]) Programma di Stoccolma — Un'Europa aperta e sicura al servizio e a tutela dei cittadini, approvato dal Consiglio europeo nel dicembre 2009.

([2]) Parere del 10 luglio 2009 sulla comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo «Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini», GU C 276 del 17.11.2009, pag. 8, punto 60.

([3]) Parere 168 del gruppo dell'articolo 29 sul futuro della vita privata, contributo congiunto alla consultazione della Commissione europea sul quadro legale per il diritto fondamentale alla protezione dei dati personali, adottato il 1º dicembre 2009.

51. Quanto detto sopra comprende inoltre ambiti in cui la Commissione è responsabile dei sistemi informativi su larga scala, quali SIS e VIS, nonché di quei casi in cui la responsabilità della Commissione è limitata allo sviluppo e al mantenimento dell'infrastruttura comune di un sistema di questo tipo, come il Sistema europeo di informazione sui casellari giudiziari (ECRIS).

52. Il grado di esattezza con cui verrà sviluppato il principio di PbD dipenderà da ogni settore e situazione particolare. Ad esempio, quando le iniziative della Commissione sono accompagnate da proposte legislative su un settore specifico delle TIC, in molti casi sarà opportuno comprendere un riferimento esplicito alla nozione di PbD applicabile alla struttura dell'applicazione/sistema di TIC particolare. Se vengono progettati piani d'azione per un ambito specifico, essi dovrebbero assicurare sistematicamente l'applicazione del quadro giuridico e più specificamente garantire che la relativa tecnologia TIC sia sviluppata tenendo in considerazione il principio della tutela della vita privata sin dalla progettazione.

53. Per quanto riguarda la ricerca, il settimo programma quadro e quelli seguenti dovrebbero essere utilizzati come strumento per sostenere progetti che mirano ad analizzare gli standard, le tecnologie e l'architettura TIC più appropriati per la vita privata e soprattutto per il principio della tutela della vita privata sin dalla progettazione. Inoltre, la PbD dovrebbe essere anche un elemento necessario da considerare in progetti TIC più ampi destinati al trattamento dei dati personali degli individui.

Ambiti di preoccupazione specifica

54. In alcuni casi, a causa dei rischi particolari per la protezione della vita privata e dei dati degli individui o a causa di altri fattori (resistenza del mercato a fornire prodotti con PbD, domanda dei consumatori, ecc) può essere necessario definire misure di tutela della vita privata sin dalla progettazione più esplicite e più specifiche, che devono essere incorporate in un determinato tipo di prodotto/tecnologia di informazione e comunicazione, sia esso all'interno o meno di strumenti legislativi.

55. Il GEPD ha individuato diversi ambiti (RFID, social networking e applicazioni di browser) che meritano, secondo il suo parere, in questa fase, un'attenta considerazione da parte della Commissione e il maggiore intervento sul campo auspicato in precedenza. Questi tre ambiti vengono discussi ulteriormente nel prosieguo.

V. **IDENTIFICAZIONE A RADIOFREQUENZA — RFID**

56. Le etichette RFID possono essere integrate negli oggetti, negli animali e nelle persone. Possono essere utilizzate per raccogliere e memorizzare dati personali quali le cartelle cliniche, per seguire i movimenti delle persone o per tracciare dei profili del loro comportamento per diversi scopi. Ciò può essere fatto senza che gli individui ne siano consapevoli ([1]).

57. Garanzie efficaci per quanto riguarda la protezione dei dati, la vita privata e tutte le dimensioni etiche collegate sono fondamentali per la fiducia pubblica nell'identificazione a radiofrequenza e per un futuro «Internet degli oggetti». Soltanto allora la tecnologia potrà offrire i suoi numerosi benefici economici e sociali.

V.1. **Le lacune del quadro legale sulla protezione dei dati applicabile**

58. La direttiva sulla protezione dei dati e la direttiva e-privacy si applicano alla raccolta di dati realizzata attraverso applicazioni RFID ([2]). Esse richiedono, tra l'altro, che vengano messe in atto adeguate tutele della vita privata allo scopo di far funzionare applicazioni di RFID ([3]).

59. Tuttavia, questo quadro legale non affronta completamente tutte le preoccupazioni relative alla protezione dei dati e alla vita privata sollevate da questa tecnologia. Questo perché le direttive non sono sufficientemente dettagliate riguardo al tipo di tutele che dovrebbero essere

([1]) RFID sta per dispositivo di identificazione a radiofrequenza. I principali componenti della tecnologia o infrastruttura di identificazione a radiofrequenza sono un'etichetta (ad esempio un microchip), un lettore e un'applicazione collegata alle etichette e ai lettori tramite un programma di connessione (middleware) e l'elaborazione dei dati prodotti. L'etichetta è composta da un circuito elettronico che archivia i dati e da un'antenna che comunica i dati tramite le onde radio. Il lettore possiede un'antenna e un demodulatore che traduce le informazioni analogiche in ingresso dal collegamento radio in dati digitali. Le informazioni possono quindi essere inviate tramite reti a banche dati e server per essere elaborate da un computer.

([2]) La direttiva e-privacy fa riferimento alla radiofrequenza nell'articolo 3: «La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati». Ciò viene integrato dal considerando 56: «Il progresso tecnologico permette lo sviluppo di nuove applicazioni basate su dispositivi per la raccolta e l'identificazione dei dati, come ad esempio i dispositivi senza contatto che utilizzano le radiofrequenze. Gli RFID (Radio Frequency Identification Devices, dispositivi di identificazione a radiofrequenza), ad esempio, utilizzano le radiofrequenze per rilevare dati da etichette identificate in modo univoco, che possono in seguito essere trasferiti attraverso le reti di comunicazione esistenti. Un ampio utilizzo di tali tecnologie può generare significativi vantaggi economici e sociali e, di conseguenza, apportare un contributo prezioso al mercato interno, sempre che il loro utilizzo risulti accettabile per la popolazione. A tal fine, è necessario garantire la tutela di tutti i diritti fondamentali degli individui, compreso il diritto alla vita privata e alla tutela dei dati a carattere personale. Quando tali dispositivi sono collegati a reti di comunicazione elettronica accessibili al pubblico, o usano servizi di comunicazione elettronica come infrastruttura di base, è opportuno che si applichino le disposizioni pertinenti della direttiva 2002/58/CE (direttiva relativa alla vita privata e alle comunicazioni elettroniche), in particolare quelle sulla sicurezza, sui dati relativi al traffico e alla localizzazione e sulla riservatezza».

([3]) Ad esempio, l'articolo 17 della direttiva sulla protezione dei dati impone un obbligo di attuare le misure tecniche e organizzative adeguate per proteggere i dati personali contro la distruzione accidentale o illegale o contro la divulgazione non autorizzata.

attuate nelle applicazioni di RFID. Le regole esistenti devono essere integrate con regole supplementari che impongono tutele specifiche, che rendono obbligatorio soprattutto includere soluzioni tecniche (tutela della vita privata fin dalla progettazione) nella tecnologia RFID. Ciò vale per le etichette che memorizzano le informazioni personali, che dovrebbero essere dotate di «comandi kill» e per l'uso della crittografia in etichette che memorizzano determinati tipi di informazioni personali.

V.2. **Primo passo: autoregolamentazione**

60. Nel marzo 2007, la Commissione ha adottato una comunicazione ([1]) che riconosce, tra l'altro, la necessità di un orientamento dettagliato sull'attuazione pratica del dispositivo di identificazione a radiofrequenza (RFID) e la desiderabilità di adottare criteri di progettazione per evitare rischi alla riservatezza e alla sicurezza.

61. Per raggiungere questi obiettivi, nel maggio 2009, la Commissione ha adottato una raccomandazione sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate su RFID ([2]). Per quanto riguarda le applicazioni basate su RFID nell'ambito della vendita al dettaglio, è necessaria la disattivazione della targhetta presso il punto di vendita tranne qualora le singole persone abbiano dato il proprio consenso. Ciò si applica in tutti i casi ad eccezione di quando una valutazione dell'impatto della protezione della vita privata e dei dati personali dimostri che le etichette non rappresentano una possibile minaccia alla protezione della vita privata e dei dati personali, nel qual caso rimarranno operative dopo il punto di vendita a meno che le singole persone, a titolo gratuito, non decidano altrimenti.

62. Il GEPD concorda con l'approccio della Commissione di utilizzare strumenti di autoregolamentazione. Tuttavia, come descritto ulteriormente di seguito, è concepibile che l'autoregolamentazione non produca i risultati previsti; pertanto fa appello alla Commissione affinché sia pronta ad adottare misure alternative.

V.3. **Ambiti di preoccupazione e possibili misure aggiuntive in caso di fallimento dell'autoregolamentazione**

63. Il GEPD è preoccupato che le organizzazioni che si occupano del funzionamento delle applicazioni basate su RFID nel settore della vendita al dettaglio possano sottovalutare la possibilità che le etichette RFID vengano monitorate da terze parti indesiderate. Tale monitoraggio potrebbe rivelare dati personali archiviati nella targhetta (se presente), tuttavia potrebbe anche consentire a una terza parte di seguire le mosse di una persona o riconoscerla nel tempo semplicemente utilizzando gli identificatori esclusivi contenuti in una o più etichette trasportate da tale persona, in un ambiente che può persino trovarsi al di fuori del perimetro operativo dell'applicazione RFID. Inoltre, è preoccupato che gli operatori delle applicazioni a radiofrequenza possano essere tentati di non rispettare le regole e commettere eccezioni, lasciando operativa la targhetta all'uscita dal punto di vendita.

64. Se si verifica quanto sopra, potrebbe essere troppo tardi per mitigare i rischi per la protezione della vita privata e dei dati personali e le singole persone potrebbero già averne risentito. Inoltre, data la natura dell'autoregolamentazione, le autorità nazionali incaricate dell'applicazione della legge potrebbero trovarsi in una posizione svantaggiata nel momento in cui richiedono alle organizzazioni che si occupano del funzionamento delle applicazioni RFID di adottare una specifica *privacy by design* (PbD, tutela della vita privata sin dalla progettazione).

65. Alla luce di quanto sopra, il GEPD fa appello alla Commissione affinché sia pronta a proporre strumenti legislativi di regolamentazione delle questioni principali dell'uso dell'RFID qualora fallisca l'attuazione efficace del quadro giuridico esistente. La valutazione della Commissione non dovrebbe essere indebitamente posposta; la sua posposizione presenterebbe dei rischi per le singole persone e sarebbe anche controproduttiva per il settore, dato che le incertezze legali sono troppo elevate e i problemi correlati potrebbero essere più difficili e costosi da correggere.

66. Tra le misure che potrebbe essere necessario proporre, il GEPD raccomanda la prescrizione del principio di inclusione presso il punto di vendita conformemente al quale tutte le etichette RFID affisse ai prodotti di consumo verrebbero disattivate al punto di vendita per impostazione predefinita. Potrebbe non essere necessario o appropriato per la Commissione specificare la tecnologia concreta da utilizzare. Al contrario, la legge dell'Unione europea deve stabilire l'obbligo legale di ottenere il consenso di inclusione, lasciando decidere agli operatori la modalità di adempimento della prescrizione.

V.4. **Ulteriori questioni da considerare: governance dell'Internet degli oggetti**

67. Le informazioni prodotte dalle etichette RFID, ad esempio le informazioni sul prodotto, possono eventualmente essere interconnesse in una rete globale di infrastruttura di comunicazione. A ciò si fa in genere riferimento con l'espressione «Internet of things» (Internet degli oggetti). Le questioni relative alla protezione della vita privata e dei dati personali sorgono poiché gli oggetti del mondo reale possono essere identificati da etichette RFID che oltre alle informazioni sul prodotto possono includere dati personali.

68. Esistono numerose questioni aperte riguardo a chi gestirà l'archivio delle informazioni correlate agli elementi etichettati. Come sarà organizzato? Chi vi avrà accesso? Nel giugno 2009, la Commissione ha approvato una comunicazione sull'Internet degli oggetti ([3]) che ha individuato esplicitamente i potenziali problemi di questo fenomeno relativamente alla protezione della vita privata e dei dati personali.

([1]) Comunicazione della Commissione del 15.3.2007 al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sull'identificazione a radiofrequenza (RFID) in Europa: verso un quadro politico, COM(2007) 96 definitivo.

([2]) Raccomandazione della Commissione, del 12.5.2009, sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza [C(2009) 3200 definitivo].

([3]) Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sull'Internet degli oggetti — Un piano d'azione per l'Europa, 18.6.2009, COM(2009) 278 definitivo.

69. Il GEPD vorrebbe sottolineare alcune delle questioni sollevate dalla comunicazione che, a suo parere, meritano un'attenzione particolare mentre si sviluppa l'Internet degli oggetti. In primo luogo, la necessità di un'architettura decentralizzata potrebbe facilitare l'affidabilità ed esecutività del quadro giuridico dell'UE. In secondo luogo, dovrebbero essere salvaguardati quanto più possibile i diritti delle singole persone a non essere rintracciate. In altri termini, dovrebbero esserci casi molto limitati in cui le persone vengono rintracciate tramite le etichette RFID senza il loro consenso. Tale consenso dovrebbe essere esplicito. Ciò è noto in genere come il «silence of chips» (disattivare i chip) e il «diritto di essere lasciato in pace». Infine, nel progettare l'Internet degli oggetti, il principio della tutela della vita privata sin dalla progettazione dovrebbe costituire un principio guida. Questo richiederebbe, ad esempio, di progettare applicazioni RFID concrete dotate di meccanismi incorporati per fornire il controllo agli utenti con impostazioni di riservatezza predefinite.

70. Il GEPD prevede di essere consultato mentre la Commissione mette a punto le azioni previste nella comunicazione, in particolare la stesura del progetto della comunicazione sulla riservatezza e la fiducia nella società dell'informazione totale.

VI. **RETI SOCIALI E NECESSITÀ DI IMPOSTAZIONI DI RISERVATEZZA PREDEFINITE**

71. Le reti sociali sono la novità del momento. La loro popolarità sembra avere superato quella dell'e-mail; mettono le persone in contatto con altre che condividono interessi e/o attività simili. Le persone possono mettere i loro profili online e condividere documenti multimediali quali video, foto, musica e i loro profili di carriera.

72. I giovani hanno adottato rapidamente l'abitudine di partecipare alla creazione di reti sociali e questa tendenza continua. L'età media degli utenti di Internet in Europa è diminuita negli ultimi anni: i bambini di 9-10 anni ora si collegano più volte alla settimana; i ragazzi di 12-14 anni si collegano quotidianamente, spesso da una a tre ore al giorno.

VI.1. **Reti sociali e quadro giuridico applicabile per la protezione della vita privata e dei dati personali**

73. Lo sviluppo delle reti sociali ha consentito agli utenti di pubblicare su Internet informazioni personali e riguardanti terze parti. Nel fare ciò, conformemente al gruppo dell'articolo 29 ([1]), gli utenti di Internet agiscono come responsabili del trattamento di dati, in base all'articolo 2, lettera d) della direttiva sulla protezione dei dati, per i dati che pubblicano online ([2]). Tuttavia, nella maggior parte dei casi tale elaborazione rientra nell'eccezione di cui all'articolo 3.2 della direttiva. Al contempo, i servizi di creazione di reti sociali sono considerati responsabili del trattamento di dati in quanto procurano i mezzi per l'elaborazione dei dati dell'utente e forniscono tutti i servizi di base correlati alla gestione degli utenti (ad esempio, registrazione ed eliminazione degli account).

74. In termini legali ciò significa che gli utenti Internet e i servizi di social network condividono la responsabilità congiunta per l'elaborazione dei dati personali come «responsabili del trattamento di dati» ai sensi dell'articolo 2, lettera d) della direttiva, anche se a livelli diversi e con serie di obblighi diversi.

75. Di conseguenza, gli utenti dovrebbero conoscere e comprendere che elaborando le proprie informazioni personali e quelle degli altri, rientrano nelle disposizioni della legislazione dell'UE in materia di protezione dei dati che richiede, tra l'altro, l'ottenimento del consenso informato delle persone alle quali si riferiscono direttamente le informazioni pubblicate e la concessione a tali persone del diritto di rettifica, obiezione ecc. Allo stesso modo, i servizi di social network, devono, tra l'altro, attuare misure tecniche e organizzative adeguate per impedire l'elaborazione non autorizzata delle informazioni, tenendo conto dei rischi rappresentati dall'elaborazione e della natura dei dati. Ciò a sua volta significa che i servizi di social network dovrebbero assicurare impostazioni predefinite non lesive della sfera privata, tra cui impostazioni che limitano l'accesso al profilo ai soli contatti espressamente prescelti dall'utente stesso. Le impostazioni dovrebbero richiedere anche il consenso affermativo prima che un qualsiasi profilo diventi accessibile a terze parti e i profili ad accesso limitato non dovrebbero essere reperibili dai motori di ricerca interni.

76. Sfortunatamente, esiste un divario tra le prescrizioni legali e la conformità effettiva. Sebbene in termini legali gli utenti di Internet siano considerati responsabili del trattamento di dati e siano vincolati dal quadro giuridico dell'UE in materia di protezione della vita privata e dei dati personali, in realtà, essi sono spesso inconsapevoli di questo ruolo. In termini generali, hanno una scarsa comprensione del fatto che stanno elaborando dati personali e che nella pubblicazione di tali informazioni sono impliciti rischi correlati alla protezione della vita privata e dei dati personali. I giovani in particolare pubblicano contenuti online sottovalutando le conseguenze per se stessi e per gli altri, ad esempio, nel contesto della loro successiva iscrizione presso istituti di insegnamento o delle loro future candidature di lavoro.

([1]) Cfr il parere 5/2009 adottato dal gruppo di lavoro WP 163 sull'articolo 29 sui social network online, adottato il 12 giugno 2009.

([2]) «Controllore» sta a significare la persona fisica o giuridica, l'autorità pubblica, l'agenzia o un qualsiasi altro ente che da solo o congiuntamente ad altri stabilisce gli scopi e i mezzi dell'elaborazione dei dati personali; laddove gli scopi e i mezzi dell'elaborazione sono stabiliti da leggi o regolamenti nazionali o comunitari, il controllore o i criteri specifici per la sua nomina possono essere designati dalla legge nazionale o comunitaria.

77. Al contempo, i provider di social network spesso preselezionano impostazioni predefinite basate su opzioni di esclusione, agevolando in tal modo la divulgazione di informazioni personali. Alcuni consentono la reperibilità dei profili tramite i comuni motori di ricerca per impostazione predefinita. Ciò suscita interrogativi sul fatto che le singole persone abbiano effettivamente acconsentito alla divulgazione di tali informazioni oltre che sulla verifica della conformità dei social network con l'articolo 17 della direttiva (sopra descritta) che richiede ai provider di attuare misure tecniche e organizzative adeguate per impedire l'elaborazione non autorizzata.

VI.2. **Rischi generati dai social network e azioni suggerite per affrontarli**

78. Quanto sopra aumenta il rischio per la protezione della vita privata e dei dati personali. Espone gli utenti di Internet e quelli i cui dati sono stati pubblicati a violazioni palesi della protezione della loro vita privata e dei dati personali.

79. In questo contesto, la questione che dovrebbe affrontare la Commissione è che cosa si dovrebbe e si potrebbe fare per rimediare alla situazione. Questo parere non fornisce una risposta completa alla domanda, al contrario suggerisce un certo numero di consigli per prenderla ulteriormente in considerazione.

Investire nell'istruzione degli utenti di Internet

80. Il primo suggerimento consiste nell'investire nell'istruzione dell'utente. A questo proposito, le istituzioni dell'UE e le autorità nazionali dovrebbero investire nell'istruzione e nella sensibilizzazione in merito alle minacce poste dai siti Internet dei social network. Ad esempio, la DG Società dell'Informazione e media si è occupata della gestione del *Safer Internet Programme*, (programma per un'Internet più sicura) che mira ad attribuire più opportunità ai bambini e ai giovani e a tutelarli, ad esempio, mediante attività di sensibilizzazione ([1]). Recentemente, le istituzioni dell'UE hanno lanciato la campagna «Think before you post» (Prima di postare pensa) per sensibilizzare i giovani riguardo ai rischi di condivisione delle informazioni personali con persone sconosciute.

81. Il GEPD incoraggia la Commissione a continuare a sostenere questo tipo di attività. Tuttavia, gli stessi provider di social network dovrebbero svolgere un ruolo attivo, poiché ad essi spetta la responsabilità giuridica e sociale di istruire gli utenti riguardo alle modalità di utilizzo dei loro servizi in un modo sicuro e non lesivo della sfera privata.

82. Come descritto in precedenza, quando si «postano» informazioni sui social network, le informazioni possono essere rese disponibili per impostazione predefinita in numerosi modi diversi. Ad esempio, le informazioni possono essere disponibili al pubblico in generale, incluso ai motori di ricerca, che possono elencarle e pertanto fornire collegamenti diretti ad esse. D'altro canto, le informazioni possono essere limitate ad «amici selezionati» o possono essere mantenute completamente riservate. Naturalmente, le autorizzazioni del profilo e la terminologia utilizzata variano da sito a sito.

83. Ciononostante, come delineato in precedenza, pochissimi utenti dei servizi di social network sanno come controllare l'accesso alle informazioni che «postano», ancora meno sono in grado di modificare le impostazioni di riservatezza predefinite. Le impostazioni di riservatezza, in genere, rimangono inalterate poiché gli utenti non sono consapevoli delle implicazioni del fatto di non averle modificate o non sanno come farlo. Nella maggior parte dei casi, tuttavia, il fatto di non avere modificato le impostazioni di riservatezza non significa che le persone abbiano preso la decisione informata di accettare lo scambio di informazioni. In questo contesto, è particolarmente importante che le terze parti, quali, ad esempio, i motori di ricerca, non creino collegamenti con i singoli profili, presupponendo che gli utenti abbiano acconsentito per impostazione predefinita (non modificando le impostazioni di riservatezza) a rendere disponibili le informazioni senza limitazioni.

84. L'istruzione degli utenti potrebbe essere d'aiuto per rimediare a questa situazione, tuttavia essa non può funzionare da sola. Come raccomanda il gruppo dell'articolo 29 nel suo parere sui social network, i provider di social network dovrebbero offrire impostazioni predefinite di riservatezza gratuite non lesive della sfera privata. Ciò renderebbe gli utenti più sensibili riguardo alle proprie azioni e, consentirebbe loro di operare scelte migliori in merito all'intenzione o meno di condividere informazioni e riguardo ai destinatari di tali informazioni.

Ruolo dell'autoregolamentazione

85. La Commissione ha stipulato un accordo con venti provider di social network noti come «Safer Social Networking Principles for the EU» (Principi più sicuri in materia di socializzazione in rete nell'UE) ([2]). Lo scopo dell'accordo è di migliorare la sicurezza dei minori durante l'utilizzo dei siti di social network in Europa. Tali principi includono numerose delle prescrizioni derivate dall'applicazione del quadro giuridico di protezione dei dati sopra descritto. Essi includono, ad esempio, la prescrizione di aumentare le opportunità di controllo a disposizione degli utenti tramite strumenti e tecnologie, per assicurare loro di poter controllare l'uso e la diffusione delle proprie informazioni personali. Viene inclusa anche la necessità di fornire impostazioni di riservatezza per impostazione predefinita.

86. Agli inizi del gennaio 2010, la Commissione ha reso disponibili i risultati di una relazione che valuta l'applicazione dei principi ([3]). Il GEPD è preoccupato che questa relazione mostri che, sebbene alcuni passi siano stati intrapresi, ne restino ancora molti altri da fare. La relazione

([1]) Le informazioni su tale programma sono disponibili all'indirizzo: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) I principi sono disponibili all'indirizzo: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) La relazione sulla valutazione dell'attuazione dei Safer Social Network Principles for the EU è disponibile all'indirizzo: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

ha riscontrato, ad esempio, problemi riguardanti la comunicazione delle misure di sicurezza e gli strumenti disponibili sui siti. Ha riscontrato inoltre che meno della metà dei firmatari dell'accordo limita l'accesso dei profili dei minori ai soli loro amici.

Esigenza di impostazioni di riservatezza predefinite obbligatorie

87. In questo contesto, la questione chiave è se le misure politiche aggiuntive sono necessarie per assicurare che i social network impostino i loro servizi con impostazioni predefinite di riservatezza. Questa questione è stata sollevata dal precedente commissario della Società dell'Informazione Viviane Reding, la quale ha sottolineato che potrebbe essere necessaria una legislazione [1]. Lungo le stesse linee di discorso, il Comitato economico e sociale europeo ha affermato che parallelamente all'autoregolamentazione dovrebbero essere imposti per legge standard minimi di protezione [2].

88. Come osservato in precedenza, l'obbligo per i provider di social network di attuare impostazioni di riservatezza predefinite può essere dedotto indirettamente dall'articolo 17 della direttiva sulla protezione dei dati [3] che obbliga i responsabili del trattamento dei dati a intraprendere misure tecniche e organizzative adeguate («both at the time of the design of the processing system and at the time of the processing itself») (sia al momento della progettazione del sistema di elaborazione che durante la fase di elaborazione stessa) per mantenere la sicurezza ed evitare l'elaborazione non autorizzata, tenendo conto dei rischi rappresentati dall'elaborazione e della natura dei dati.

89. Tuttavia, questo articolo è di gran lunga troppo generico e manca di specificità, anche in questo contesto. Non afferma chiaramente che cosa si intenda per misure tecniche e organizzative adeguate nel contesto dei social network. Pertanto, la situazione attuale è caratterizzata da un'incertezza giuridica tale da causare problemi sia ai legislatori sia alle persone la cui vita privata e dati personali non sono interamente protetti.

90. Alla luce di quanto sopra, il GEPD insiste presso la Commissione affinché prepari una legislazione che includa, come prescrizione minima, l'obbligo generale di richiedere impostazioni predefinite di riservatezza, unite a prescrizioni più precise:

a) prescrivere impostazioni che limitino l'accesso ai profili utente ai soli contatti selezionati dall'utente stesso. Le impostazioni dovrebbero anche richiedere il consenso affermativo dell'utente prima che qualsiasi profilo sia accessibile alle terze parti;

b) prescrivere che i profili d'accesso limitati non siano reperibili tramite motori di ricerca interna o esterna.

91. Oltre al fatto di prescrivere impostazioni predefinite obbligatorie per la riservatezza, rimane aperta la questione se possono essere adeguate anche la protezione dei dati specifica aggiuntiva e altre misure (ad esempio, riguardanti la protezione dei minori). Ciò solleva la questione più ampia se sia adeguato o meno creare un quadro specifico per questi tipi di servizi che, oltre a prevedere impostazioni di riservatezza obbligatorie, regolerebbero altri aspetti. Il GEPD ha chiesto alla Commissione di prendere in considerazione tale questione.

VII. **IMPOSTAZIONI PREDEFINITE DI RISERVATEZZA DEL BROWSER PER GARANTIRE IL CONSENSO INFORMATO PER RICEVERE ANNUNCI**

92. I provider di reti di inserzioni utilizzano cookie e altri dispositivi per eseguire il monitoraggio del comportamento dei singoli utenti quando navigano su Internet al fine di catalogare i loro interessi e creare profili. Queste informazioni vengono quindi utilizzate per inviare le loro inserzioni mirate [4].

VII.1. **Sfide e rischi rimanenti nell'ambito del quadro giuridico attuale di protezione dei dati e della riservatezza**

93. La presente elaborazione è coperta dalla direttiva sulla protezione dei dati (quando sono coinvolti i dati personali) e anche dall'articolo 5.3 della direttiva e-Privacy. Questo articolo richiede specificatamente che l'utente venga informato e che gli venga concessa l'opportunità di reagire accettando o rifiutando l'archiviazione di dispositivi quali, ad esempio, i cookie ecc sul suo computer o su un altro dispositivo [5].

94. Fino ad oggi, i provider di reti di inserzioni hanno fatto affidamento sulle impostazioni del browser e su politiche in materia di riservatezza per informare gli utenti e consentire loro di accettare o rifiutare i cookie. Essi hanno

[1] Viviane Reding, membro della Commissione europea responsabile per la Società dell'Informazione e media, *think before you post! how to make social networking sites safer for children and teenagers?* (Pensa prima di postare! Come fare per rendere più sicura la socializzazione in rete per i bambini e gli adolescenti?), Safer Internet Day Strasburgo, 9 febbraio 2010.

[2] Parere del Comitato economico e sociale europeo sull'impatto dei siti di social network sui cittadini/consumatori, 4 novembre 2009.

[3] Ampliamento anche al punto 33 del presente documento.

[4] I *tracking cookies* (cookie traccianti) sono documenti di testo di piccole dimensioni contenenti un identificatore esclusivo. In genere, i provider di reti di inserzioni (otre agli operatori o editori di siti Internet) inseriscono i cookie nel disco rigido dei visitatori del sito, in particolare nel browser degli utenti di Internet, quando gli utenti effettuano il primo accesso ai siti Internet pubblicando inserzioni che fanno parte della loro rete. Il cookie consente a un provider di rete di riconoscere un precedente visitatore che accede di nuovo a quel sito Internet o che visita un qualsiasi sito Internet partner della rete di inserzioni. Tali visite ripetute consentono al provider della rete di inserzioni di creare un profilo del visitatore.

[5] L'articolo 5, paragrafo 3 della direttiva e-Privacy è stato modificato di recente per rafforzare la protezione contro l'intercettazione delle comunicazioni degli utenti attraverso l'uso, ad esempio, di spyware e cookie archiviati sul computer di un utente o su un altro dispositivo. Ai sensi della nuova direttiva agli utenti dovrebbero essere offerte informazioni migliori e modi più semplici di controllare se vogliono archiviare cookie nei loro terminali.

spiegato nelle politiche di riservatezza degli editori come scegliere opzioni di esclusione per non ricevere cookie in generale o per accettarli caso per caso. Nel fare ciò, intendono essere conformi al loro obbligo di offrire agli utenti il diritto di rifiutare i cookie.

95. Sebbene teoricamente questo metodo (tramite il browser) possa in effetti prevedere in modo efficiente un consenso informato significativo, la realtà è molto diversa. In generale, agli utenti manca la comprensione di base della raccolta di qualsiasi tipo di dati, che è ancora più scarsa se si tratta di terze parti, nonché del valore di tali dati, degli usi che ne vengono fatti, di come funziona la tecnologia e, ancora più in particolare, di come e in quali casi scegliere le opzioni di esclusione. I passi che devono compiere gli utenti per scegliere le opzioni di esclusione non appaiono solo complicati ma anche eccessivi (in primo luogo, occorre impostare il browser per accettare i cookie, quindi in un secondo momento è possibile esercitare l'opzione di esclusione).

96. Di conseguenza, in pratica un numero molto limitato di persone esercita l'opzione di esclusione, non in seguito a una decisione informata di accettare *behavioural advertisement* (pubblicità comportamentale), quanto piuttosto perché non si rende conto che evitando di usare l'opzione di esclusione in realtà sta fornendo inconsapevolmente il suo consenso.

97. Pertanto, in termini giuridici, l'articolo 5, paragrafo 3 della direttiva e-Privacy prevede una protezione legale efficace, in pratica, si ritiene che gli utenti di Internet abbiano fornito il loro consenso a essere monitorati allo scopo di inviare loro pubblicità comportamentale quando, in effetti, nella maggior parte se non addirittura nella totalità dei casi, essi sono completamente inconsapevoli del fatto di essere monitorati.

98. Il gruppo dell'articolo 29 sta preparando un parere, atteso favorevolmente, che mira a chiarire le prescrizioni legali per svolgere attività di pubblicità comportamentale. Tuttavia, l'interpretazione potrebbe non essere sufficiente di per sé per risolvere questa situazione e potrebbe essere necessario per l'Unione europea intraprendere ulteriori misure.

VII.2. **Necessità di ulteriori azioni, in particolare per introdurre prescrizioni in materia di impostazioni predefinite di riservatezza obbligatorie**

99. Come descritto in precedenza, i browser web, in genere, consentono un certo livello di controllo su determinati tipi di cookie. Attualmente, le impostazioni predefinite della maggior parte dei browser web accettano tutti i cookie. In altri termini, per impostazione predefinita, i browser sono regolati in modo da accettare tutti i cookie, indipendentemente dallo scopo del cookie stesso. Solo se l'utente modifica le impostazioni dell'applicazione del browser per rifiutare i cookie, cosa che come è stato osservato in precedenza, fa un numero molto esiguo di utenti, sarà possibile non ricevere cookie. Inoltre, non è previsto un *privacy wizard* (generatore di clausole sulla vita privata) durante la prima installazione o durante le installazioni aggiornamento delle applicazioni del browser.

100. Un modo per mitigare il problema precedente sarebbe se i browser fossero provvisti di impostazioni predefinite di riservatezza. In altri termini, se fossero dotati dell'impostazione di «non accettazione dei cookies di terze parti». Per integrare e rendere più efficace questa impostazione, i browser dovrebbero richiedere all'utente di eseguire un generatore di clausole sulla vita privata quando installano il browser per la prima volta o quando installano gli aggiornamenti. Esiste l'esigenza di informazioni più chiare e capillari sui tipi di cookie e sull'utilità di alcuni di essi. Gli utenti che desiderano essere monitorati allo scopo di ricevere pubblicità dovrebbero essere debitamente informati e dovrebbe essere necessario per loro modificare le impostazioni del browser. Ciò consentirebbe loro un migliore controllo sulla propria vita privata e sui dati personali. Secondo il GEPD, si tratterebbe di un modo efficace di rispettare e preservare il consenso degli utenti [1].

101. Tenendo conto, da un lato, della natura diffusa del problema, in altri termini, del numero di utenti di Internet attualmente monitorati sulla base di un consenso che è illusorio e, dall'altra, dell'entità dell'interesse in gioco, la necessità di salvaguardia aggiuntiva diventa più impellente. L'attuazione del principio della PbD nelle applicazioni dei browser web potrebbe fare una differenza sostanziale nel consentire alle singole persone di mantenere il controllo sulle prassi di raccolta dati utilizzate a scopi pubblicitari.

102. Per queste ragioni, il GEPD insiste presso la Commissione affinché essa consideri misure che richiedano impostazioni di riservatezza predefinite obbligatorie nei browser e la fornitura delle informazioni rilevanti.

VIII. **ALTRI PRINCIPI CHE MIRANO ALLA PROTEZIONE DELLA VITA PRIVATA E DEI DATI PERSONALI DELLE SINGOLE PERSONE**

103. Il principio della PbD possiede un grande potenziale per migliorare la protezione della vita privata e dei dati personali delle singole persone, la progettazione e l'attuazione nell'ambito della legge dei principi di complementarità per assicurare ai consumatori che la fiducia nei TIC è necessaria. In questo contesto, il GEPD affronta il principio di responsabilità e il complemento di un quadro obbligatorio di violazione della sicurezza applicabile a settori diversi.

VIII.1. **Il principio di responsabilità per assicurare la conformità con il principio di riservatezza in base alla progettazione**

104. Il documento del gruppo dell'articolo 29 intitolato «Future of Privacy» [2] raccomanda di includere il principio di responsabilità nella direttiva sulla protezione dei dati.

---

[1] Al contempo, il GEPD è consapevole che ciò non risolverebbe completamente il problema dal momento che esistono cookie che non possono essere controllati tramite il browser, ad esempio, i cosiddetti *flash cookies*. In questo caso, gli sviluppatori di browser dovrebbero integrare le impostazioni predefinite per controlli flash all'interno dei loro controlli di cookie nelle versioni aggiornate dei nuovi browser.

[2] Parere 168 del gruppo sull'articolo 29 sul *The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data,* (Il futuro della protezione della vita privata, contributo congiunto alla consultazione della Commissione europea sul quadro giuridico del diritto fondamentale alla protezione dei dati personali) adottato il 1º dicembre 2009.

Questo principio, che è riconosciuto in alcuni strumenti di protezione dei dati multinazionali ([1]), richiede che le organizzazioni attuino processi per essere conformi alle leggi esistenti e mettano a punto metodi per la valutazione e la dimostrazione della conformità con la legge e gli altri strumenti vincolanti.

105. Il GEPD sostiene interamente la raccomandazione del gruppo dell'articolo 29. Considera che questo principio sarà estremamente rilevante per promuovere l'applicazione effettiva dei principi e degli obblighi di protezione dei dati. La responsabilità richiederà ai responsabili del trattamento di dati di dimostrare che sia stato messo in atto il meccanismo necessario per conformarsi con la legislazione di protezione de dati applicabile. Ciò dovrebbe contribuire all'attuazione efficace della riservatezza in base alla progettazione nelle tecnologie TIC come elemento particolarmente adatto per mostrare responsabilità.

106. Per misurare e dimostrare la responsabilità, i responsabili del trattamento dei dati potrebbero utilizzare procedure interne e terze parti che eseguano audit o altri tipi di controlli e verifiche al termine dei quali conferire marchi o riconoscimenti. In questo contesto, il GEPD insiste presso la Commissione affinché consideri se, in aggiunta a un principio di responsabilità generale, possa essere utile richiedere per legge misure di responsabilità specifiche quali la necessità di produrre valutazioni dell'impatto sulla protezione della vita privata e dei dati personali e in che circostanze.

VIII.2. **Violazione della sicurezza: completamento del quadro legale**

107. Le modifiche dell'ultimo anno alla direttiva e-Privacy hanno introdotto un requisito per notificare le violazioni di dati alle persone vittima della violazione nonché alle autorità pertinenti. Una violazione dei dati è generalmente definita come qualsiasi violazione che conduca alla distruzione, perdita, divulgazione ecc. di dati personali trasmessi, archiviati o elaborati altrimenti in connessione con il servizio. La notifica alle singole persone sarà richiesta se la violazione dei dati può avere conseguenze negative sulla riservatezza o sui dati personali. In questo caso la violazione potrebbe condurre a usurpazione d'identità, umiliazione grave o danno alla reputazione. Sarà necessaria la notifica alle autorità pertinenti per ogni violazione di dati, indipendentemente dal fatto che sussista un rischio per le singole persone.

Applicazione degli obblighi di sicurezza tra settori

108. Sfortunatamente tale obbligo si applica solo ai fornitori di servizi di comunicazioni elettroniche pubblicamente disponibili, quali le compagnie telefoniche, i provider di accesso a Internet, i provider di webmail, ecc. Il GEPD insiste presso la Commissione affinché avanzi proposte sulla violazione della sicurezza applicabile tra diversi settori. Per quando riguarda il contenuto di tale quadro, il GEPD considera che il quadro giuridico della violazione della sicurezza adottato nella direttiva e-Privacy raggiunga un equilibrio adeguato tra la protezione dei diritti delle singole persone, inclusi i loro diritti alla protezione della vita privata e dei dati personali, e l'obbligo imposto sui soggetti contemplati. Al contempo, si tratta di un quadro «con un vero mordente» dal momento che è sostenuto da significative disposizioni di carattere coercitivo, che forniscono alle autorità sufficienti poteri di indagine e sanzione in caso di non conformità.

109. Di conseguenza, il GEPD insiste presso la Commissione affinché adotti una proposta legislativa per l'applicazione di questo quadro tra settori diversi, con gli adeguamenti del caso, se necessario. Inoltre, ciò assicurerebbe l'applicazione degli stessi standard e delle medesime procedure nei diversi settori.

Completamento del quadro legale incorporato nella direttiva e-Privacy attraverso la procedura di comitato

110. La direttiva e-Privacy rivista attribuisce alla Commissione il potere di adottare misure tecniche di attuazione, ad esempio, misure dettagliate sulla notifica della violazione della sicurezza, tramite una procedura di comitato ([2]). Tale conferimento di poteri è giustificato al fine di assicurare l'attuazione e l'applicazione uniforme del quadro giuridico di violazione della sicurezza. L'attuazione omogenea agisce contribuendo ad assicurare che le singole persone in ogni parte della Comunità fruiscano dello stesso livello elevato di protezione e che i soggetti contemplati non siano oberati con requisiti di notifica divergenti.

111. La direttiva e-Privacy è stata adottata nel novembre 2009. Non sembra che vi sia alcuna ragione che giustifichi il posticipo dell'avvio dei lavori per l'adozione delle misure tecniche di attuazione. Il GEPD ha organizzato due seminari che mirano a condividere e acquisire esperienze sulla notifica della violazione dei dati. Il GEPD sarebbe lieto di condividere i risultati di questo esercizio ed è pronto a collaborare con la Commissione e le altre parti interessate nella definizione del quadro giuridico generale di violazione dei dati.

112. Il GEPD insiste presso la Commissione affinché intraprenda i passi necessari, nell'ambito di un breve quadro temporale. Prima di adottare le misure tecniche di attuazione, la Commissione deve avviare un'ampia consultazione, durante la quale vengano consultati l'ENISA, il GEPD e il gruppo dell'articolo 29. Inoltre, la consultazione deve anche includere altre «parti interessate rilevanti», in particolare al fine di uniformare i migliori mezzi tecnici ed economici di attuazione disponibili.

([1]) Linee guida dell'OCSE sulla protezione della vita privata e dei flussi transfrontalieri di dati personali, adottate il 23 settembre 1980; Dichiarazione di Madrid sulla privacy, Norme globali sulla privacy per un mondo globale, 3 novembre 2009.

([2]) La procedura di comitato comprende l'adozione di misure tecniche di attuazione tramite un comitato di rappresentanti degli Stati membri presieduti dalla Commissione. Per quanto riguarda la direttiva e-Privacy, si applica la cosiddetta procedura di regolamentazione con scrutinio, pertanto il Parlamento europeo, nonché il Consiglio possono opporsi alle misure proposte dalla Commissione. Per ulteriori informazioni cfr. http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **CONCLUSIONI**

113. La fiducia, anziché la sua assenza, è stata identificata come una questione centrale per l'emergere e il buon esito della diffusione delle tecnologie informatiche e delle comunicazioni. Se le persone non hanno fiducia nelle TIC, queste tecnologie potrebbero fallire. La fiducia nei TIC dipende da diversi fattori; assicurare che tali tecnologie non erodano i diritti fondamentali delle singole persone in materia di protezione della vita privata e dei dati personali è uno dei fattori chiave.

114. Al fine di rafforzare ulteriormente il quadro giuridico sulla protezione della vita privata e dei dati personali, i cui principi rimangono completamente validi nella società dell'informazione, il GEPD propone alla Commissione di integrare la riservatezza in base alla progettazione a diversi livelli di regolamentazione ed elaborazione di politiche.

115. Il GEPD raccomanda alla Commissione di seguire quattro mezzi d'azione:

a) propone di includere una disposizione generale sulla riservatezza in base alla progettazione nel quadro giuridico per la protezione dei dati. Tale disposizione dovrebbe essere tecnologicamente neutrale e la sua conformità dovrebbe essere obbligatoria a diversi livelli;

b) elaborare questa disposizione generale in disposizioni specifiche, dove vengano proposti strumenti giuridici specifici in settori diversi. Tali disposizioni specifiche potrebbero essere incluse ora in strumenti giuridici; sulla base dell'articolo 17 della direttiva sulla protezione dei dati (e altre leggi esistenti);

c) includere la PbD quale principio guida nell'Agenda europea del digitale;

d) inserire la PbD quale principio da tenere in considerazione nell'ambito di altre iniziative dell'UE (principalmente non legislative).

116. In tre ambiti designati delle TIC, il GEPD raccomanda alla Commissione di valutare la necessità di avanzare proposte di attuazione del principio della riservatezza in base alla progettazione in modi specifici:

a) in relazione al dispositivo di identificazione a radiofrequenza (RFID) propone misure legislative che disciplinino le questioni principali dell'utilizzo dell'RFID qualora fallisca l'attuazione efficace del quadro giuridico esistente tramite l'autoregolamentazione. In particolare, prevede l'adozione il principio di opzione di esclusione al punto di vendita in conformità col quale tutte le etichette RFID affisse ai prodotti di consumo vengono disattivate per impostazione predefinita al punto di vendita;

b) in relazione ai social network, preparare una legislazione che includa, come prescrizione minima, l'obbligo generale di impostazioni di riservatezza obbligatorie, unito a prescrizioni più precise, sulla limitazione dell'accesso ai profili utenti ai soli contatti selezionati dall'utente stesso e prescrivere che i profili ad accesso limitato non possano essere reperibili da parte dei motori di ricerca interni ed esterni;

c) in relazione alla pubblicità mirata, prendere in considerazione impostazioni predefinite del browser imposte dalla legislazione per rifiutare cookie di terze parti e rendere necessaria l'esecuzione di un *privacy wizard* (generatore di clausole sulla vita privata) alla prima installazione del browser o durante l'installazione dei successivi aggiornamenti.

117. Infine, il GEPD suggerisce alla Commissione di:

a) considerare l'attuazione del principio di responsabilità nella direttiva sulla protezione dei dati esistente; e

b) sviluppare un quadro normativo e procedurale per attuare le disposizioni in materia di notifica della violazione di sicurezza della direttiva e-Privacy ed estenderne l'applicazione in generale a tutti i responsabili del trattamento di dati.

Fatto a Bruxelles, il 18 marzo 2010.

Peter HUSTINX

Garante europeo della protezione dei dati

Parere del Garante europeo della protezione dei dati in merito alla proposta di direttiva del Parlamento europeo e del Consiglio sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

(2010/C 280/02)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

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

vista la Carta dei diritti fondamentali dell'Unione europea, in particolare l'articolo 8,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in particolare l'articolo 17,

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

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE

1. Il 3 dicembre 2008 la Commissione ha adottato una proposta di direttiva del Parlamento europeo e del Consiglio sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) (in prosieguo «la proposta») ([1]). La proposta è finalizzata a rifondere la direttiva 2002/96/CE sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) adottata il 27 gennaio 2003 (in prosieguo «la direttiva») ([2]) senza modificare le cause o le motivazioni alla base della raccolta e del riciclaggio di RAEE.

2. Diversamente da quanto prescritto dall'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 ([3]), il GEPD non è stato consultato. Agendo di propria iniziativa, il GEPD ha quindi adottato l'attuale parere in base all'articolo 41, paragrafo 2, del medesimo regolamento. Il GEPD raccomanda di includere nel preambolo della proposta un riferimento al presente parere.

3. Il GEPD, pur consapevole del fatto che questo documento giunge in una fase tardiva del processo legislativo, ritiene utile e appropriato emettere il presente parere visto che la proposta solleva questioni importanti in materia di protezione dei dati che nel testo non sono state affrontate. Il parere non intende modificare lo scopo e i contenuti principali e preponderanti della proposta, il cui «centro di gravità» ([4]) rimane la protezione dell'ambiente, bensì solo aggiungere un'ulteriore dimensione che sta divenendo sempre più rilevante per la nostra società dell'informazione ([5]).

4. Il GEPD, consapevole altresì della portata limitata della procedura di rifusione, invita nondimeno il legislatore a tener conto di tali raccomandazioni in conformità con il punto 8 dell'accordo interistituzionale sulla procedura di rifusione (che prevede la possibilità di modificare le disposizioni immutate) ([6]).

II. CONTESTO E ANTEFATTI DELLA PROPOSTA E SUA RILEVANZA PER LA PROTEZIONE DEI DATI

5. Lo scopo della proposta è aggiornare la direttiva esistente in materia di smaltimento, reimpiego e riciclo dei RAEE. Problemi di carattere tecnico, giuridico e amministrativo emersi nei primi anni di attuazione della direttiva hanno portato alla presentazione della proposta, come previsto dall'articolo 17, paragrafo 5, della direttiva.

6. Per apparecchiature elettriche ed elettroniche (AEE) si intende un'ampia gamma di prodotti che comprende una disparata serie di supporti in grado di contenere dati personali — quali le apparecchiature informatiche e di telecomunicazione (per esempio, personal computer, laptop, terminali per i servizi di comunicazione elettronica) — caratterizzati nell'attuale contesto tecno-economico da sempre più rapidi cicli d'innovazione e, data la convergenza tecnologica, dalla disponibilità di dispositivi multifunzionali. L'evoluzione dei supporti elettronici di memorizzazione è sempre più veloce, in particolare per quanto concerne la capacità di memorizzazione e le dimensioni. Di conseguenza, le forze di mercato fanno crescere in misura analoga il ricambio delle apparecchiature elettriche ed elettroniche (contenenti una grande quantità di dati personali,

([1]) COM(2008) 810 definitivo.
([2]) GU L 37 del 13.2.2003, pag. 24.
([3]) 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, GU L 8 del 12.1.2001, pag. 1.
([4]) Cfr. la sentenza della Corte del 23 febbraio 1999, causa C-42/97, *Parlamento europeo/Consiglio dell'Unione europea*, Racc. 1999, pag. I-869, punto 43.
([5]) Cfr. anche, tra l'altro, la sentenza della Corte del 30 gennaio 2001, causa C-36/98 *Spagna/Consiglio*, Racc. 2001, pag. I-779, punto 59: «Se l'esame di un atto comunitario dimostra che esso persegue una duplice finalità o che esso ha una doppia componente e se una di queste è identificabile come principale o preponderante, mentre l'altra è solo accessoria, l'atto deve fondarsi su una sola base giuridica, ossia quella richiesta dalla finalità o componente principale o preponderante».
([6]) Accordo interistituzionale, del 28 novembre 2001, ai fini di un ricorso più strutturato alla tecnica della rifusione degli atti normativi, GU C 77 del 28.3.2002, pag. 1.

spesso sensibili). Da ciò deriva non solo che i RAEE «sono considerati il flusso di rifiuti in più rapida crescita nell'UE» ([7]), bensì anche, nel caso di smaltimento inadeguato, che è prevedibile un aumento del rischio di perdita e dispersione di dati personali contenuti in questo tipo di AEE.

7. Per molto tempo le politiche dell'Unione europea sull'ambiente e sullo sviluppo sostenibile si sono concentrate sulla riduzione dello spreco di risorse naturali e sull'introduzione di misure volte a prevenire l'inquinamento.

8. In questo quadro normativo rientrano lo smaltimento, il reimpiego e il riciclo dei RAEE. Le misure introdotte mirano a evitare lo smaltimento di apparecchiature elettriche ed elettroniche insieme ai rifiuti indifferenziati, imponendo ai produttori l'obbligo di provvedere allo smaltimento secondo le modalitá previste dalla direttiva.

9. In particolare, tra le varie misure previste dalla direttiva, vale la pena mettere in luce quelle destinate al *reimpiego* (ossia le operazioni in virtù delle quali i RAEE o loro componenti sono utilizzati allo stesso scopo per cui erano stati originariamente concepiti, incluso l'uso continuativo delle apparecchiature o loro componenti riportati a punti di raccolta, a distributori, riciclatori o fabbricanti), al *riciclaggio* (ossia il ritrattamento in un processo di produzione dei materiali di rifiuto per la loro funzione originaria o per altri fini) e alla ricerca di altre forme di recupero dei RAEE in maniera tale da ridurre lo smaltimento dei rifiuti [cfr. l'articolo 1 e l'articolo 3, lettere d) ed e), della direttiva].

10. Queste operazioni, in particolare il reimpiego e il riciclaggio dei RAEE, soprattutto di apparecchiature informatiche e di telecomunicazione, possono implicare il rischio, superiore rispetto al passato, che chi raccoglie i RAEE o vende e acquista i dispositivi usati o riciclati possa avere accesso a eventuali dati personali in essi contenuti. Tali dati spesso possono essere sensibili o riferirsi a un ampio numero di soggetti.

11. Per tutti questi motivi, il GEPD ritiene urgente che tutte le parti interessate (utilizzatori e fabbricanti di AEE) siano rese edotte in merito ai rischi concernenti i dati personali, specialmente nella fase conclusiva del ciclo di vita delle AEE. In tale stadio è probabile che le AEE contengano una grande quantità di dati personali e pertanto, pur avendo un minor valore dal punto di vista economico, presumibilmente possiedono un elevato valore «intrinseco» per la persona interessata e/o per altri soggetti.

III. ANALISI DELLA PROPOSTA

III.1. Applicabilità della direttiva 95/46/CE

12. Il GEPD non muove osservazioni sull'obiettivo generale della proposta e sostiene appieno l'iniziativa adottata, volta a migliorare le politiche ecocompatibili correlate ai RAEE.

13. Ciò nondimeno, la proposta, così come la direttiva, si concentra unicamente sui rischi ambientali legati allo smaltimento dei RAEE, senza tener conto di ulteriori rischi di diversa natura per i singoli individui e/o le organizzazioni che possono insorgere a seguito delle operazioni di smaltimento, reimpiego o riciclo dei RAEE, in particolare quelli legati alla possibilità di un'acquisizione, comunicazione o diffusione improprie dei dati personali contenuti nei RAEE.

14. È importante notare che la direttiva 95/46/CE ([8]) si applica a «qualsiasi operazione o insieme di operazioni […] applicate a dati personali», compresa la loro «cancellazione o distruzione» [articolo 2, lettera b)]. Lo smaltimento delle AEE può includere operazioni di trattamento dei dati. Per questo motivo esiste una sovrapposizione tra la proposta e la testé citata direttiva, per cui le norme sulla protezione dei dati sono applicabili alle attività interessate dalla proposta.

III.2. Smaltimento dei RAEE e misure di sicurezza

15. Il GEPD intende evidenziare i rischi elevati a carico dei singoli individui e/o delle organizzazioni nella loro funzione di «responsabili del trattamento dei dati» ([9]) nel caso in cui i RAEE, in particolar modo le apparecchiature informatiche e di telecomunicazione, contengano dati personali relativi agli utenti di tali dispositivi e/o a parti terze al momento dello smaltimento. L'accesso non autorizzato o la comunicazione di tali informazioni personali, a volte consistenti in particolari categorie di dati, che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati relativi alla salute e alla vita sessuale (i cosiddetti «dati sensibili») ([10]), sono infatti in grado di influire sulla vita privata e sulla dignità della persona a cui si riferiscono, nonché su altri interessi legittimi di tali singoli individui/organizzazioni (per esempio, quelli economici).

([7]) Documento di lavoro dei servizi della Commissione che accompagna la proposta di direttiva del Parlamento europeo e del Consiglio sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) (rifusione). Valutazione dell'impatto, 3.12.2008 [COM(2008) 810 definitivo] SEC(2008) 2933, pag. 17.

([8]) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995, pag. 31.

([9]) Per la definizione di «responsabile del trattamento» cfr. l'articolo 2, lettera d), della direttiva 95/46/CE.

([10]) Cfr. l'articolo 8 della direttiva 95/46/CE.

16. In generale, il GEPD ritiene necessario sottolineare l'importanza dell'adozione di misure di sicurezza appropriate in ogni fase (da quella iniziale a quella finale) del trattamento dei dati personali, come più volte affermato in altri pareri ([11]). Ciò si applica a maggior ragione nella delicata fase in cui il responsabile del trattamento dei dati intende smaltire i dispositivi contenenti dati personali.

17. Di fatto, il rispetto delle misure di sicurezza è spesso un prerequisito per garantire efficacemente il diritto alla protezione dei dati personali.

18. Sarebbe pertanto incoerente introdurre l'obbligo di mettere in atto misure di sicurezza (talvolta costose) nel corso delle normali operazioni di trattamento dei dati personali [come previsto dall'articolo 17 della direttiva 95/46/CE, ove applicabile ([12])] e poi semplicemente omettere di prendere in considerazione l'adozione di adeguate misure di sicurezza per quanto concerne lo smaltimento dei RAEE.

19. Parimenti non sarebbe coerente, da un lato, riconoscere importanza alla questione della sicurezza del trattamento dei dati al punto da dover introdurre l'obbligo di comunicazioni delle violazioni dei dati attraverso l'articolo 2 della direttiva 2009/136/CE ([13]) e, dall'altro lato, non fornire alcuna garanzia o protezione nel corso dello smaltimento dei RAEE nonché nel caso di loro reimpiego o riciclaggio.

20. Il GEPD si rammarica del fatto che la proposta non tenga conto dei potenziali effetti dannosi dello smaltimento dei RAEE sulla protezione dei dati personali contenuti nell'apparecchiatura «usata».

21. Questo aspetto non è stato nemmeno considerato nella valutazione dell'impatto effettuata dalla Commissione ([14]), sebbene l'esperienza abbia dimostrato che la mancata adozione di misure di sicurezza appropriate nel caso dello smaltimento dei RAEE possa pregiudicare la protezione dei dati personali ([15]). Vista la complessità delle questioni (per esempio, la grande quantità di metodi legittimi, tecnologie e parti interessate nel ciclo di smaltimento dei RAEE), il GEPD è del parere che sarebbe stato opportuno effettuare una «valutazione di impatto sulla tutela della vita privata e sulla protezione dei dati» in relazione ai processi correlati allo smaltimento dei RAEE.

22. Nondimeno, il GEPD raccomanda vivamente che vengano elaborate «migliori tecniche disponibili» per la tutela della vita privata, la protezione dei dati e la sicurezza in questo settore.

23. Inoltre, nel corso della consultazione pubblica che ha preceduto la rifusione della direttiva, alcune parti interessate, in particolare le società informatiche e di comunicazione elettronica, hanno talvolta sollevato questioni concernenti la sicurezza e la protezione dei dati personali ([16]).

24. Infine, è bene evidenziare che alcune autorità nazionali preposte alla protezione dei dati hanno pubblicato linee guida per ridurre al minimo i rischi derivanti dalla mancata adozione delle necessarie misure di sicurezza, nello specifico all'atto dello smaltimento di materiali soggetti all'applicazione della direttiva ([17]).

([11]) Cfr. il parere del Garante europeo della protezione dei dati sull'agenzia per la gestione operativa dei sistemi di tecnologia dell'informazione su larga scala (GU C 70 del 19.3.2010, pag. 13), punti 46 e 47; il parere sulla proposta di direttiva concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU C 128 del 6.6.2009, pag. 20), punti 27-31.

([12]) Cfr. l'articolo 3 della direttiva.

([13]) 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.

([14]) Documento di lavoro dei servizi della Commissione che accompagna la proposta di direttiva del Parlamento europeo e del Consiglio sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) (rifusione), SEC(2008) 2933, 3.12.2008; cfr. anche Università delle Nazioni Unite, 2008 *Review of Directive 2002/96/EC on Waste Electrical and Electronic Equipment (WEEE)*, Commissione europea, Belgio, 2007, pag. 273 (http://ec.europa.eu/environment/waste/weee/pdf/final_rep_unu.pdf); *Data security is also an issue — removing personal data from a hard-drive*.

([15]) Cfr. per esempio l'articolo della BBC disponibile online *Children's files on eBay computer*, del 4 maggio 2007, che riporta l'episodio di un computer contenente dati personali concernenti l'affidamento e l'adozione di bambini venduto su eBay (http://news.bbc.co.uk/2/hi/uk_news/england/6627265.stm); cfr. anche l'articolo della BBC disponibile online *Bank customer data sold on eBay*, del 26 agosto 2008, nel quale si segnala che il disco rigido contenente dati personali relativi a un milione di clienti bancari era stato venduto su eBay (http://news.bbc.co.uk/2/hi/uk_news/7581540.stm).

([16]) Cfr. HP, *Stakeholder Consultation on the Review of Directive 2002/96/EC of the European Parliament and of the Council on Waste Electrical and Electronic Equipment (WEEE)*, pagg. 7-8; DELL (bozza di osservazioni), *WEEE Review Policy Options of the stakeholder consultation on the review of directive 2002/96/EC of the European Parliament and of the Council on Waste Electrical And Electronic Equipment (WEEE)*, pag. 2, punti 1.1 e 4, punto 1.3 (3.6.2008); Posizione e proposta di Royal Philips Electronics, *Stakeholder consultation on the Revision of the WEEE Directive*, pag. 12 (5.6.2008) (http://circa.europa.eu/Public/irc/env/weee_2008_review/library). Cfr. anche WEEE Consultation Response, *Summary of responses and Government response to fourth consultation on implementation of Directives 2002/96/EC and 2003/108/EC on Waste Electrical and Electronic Equipment*, dicembre 2006, pag. 30: «Data protection and security. Some waste management companies would like there to be some guidance issued on data protection and security, particularly in light of the fact they will be handling sensitive data» (http://www.berr.gov.uk/files/file35961.pdf).

([17]) Landesbeauftragter für Datenschutz und Informationsfreiheit Bremen, *Entwicklung eines Konzeptes zur Löschung und Datenträgervernichtung durch Behörden und Unternehmen*, 16. Mai 2007 (http://www.datenschutz-bremen.de/rtf/datenloeschung.rtf); Garante per la protezione dei dati personali, *Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali*, 13 ottobre 2008 (http://www.garanteprivacy.it/garante/doc.jsp?ID=1571514), menzionato anche nella *Twelfth Annual Report of the Article 29 Working Party on Data Protection*, 16 giugno 2009, pag. 57; cfr. anche Gruppo di lavoro internazionale sulla tutela dei dati nelle telecomunicazioni, *Recommendation on Data Protection and E-Waste*, Sofia, 12-13.3.2009 (http://www.datenschutz-berlin.de/attachments/650/675.38.14.pdf?1264671551).

25. Il GEPD ribadisce che la direttiva 95/46/CE è applicabile nella fase di smaltimento dei RAEE contenenti dati personali. I responsabili del trattamento dei dati, in particolare quelli che utilizzano dispositivi informatici e di comunicazione, devono pertanto soddisfare gli obblighi di sicurezza al fine di evitare la comunicazione o la diffusione improprie di dati personali. A tal fine e per non essere ritenuti responsabili della violazione delle norme di sicurezza, i responsabili del trattamento dei dati del settore pubblico o privato devono adottare, con la collaborazione degli incaricati aziendali della protezione dei dati (ove presenti), politiche adeguate per lo smaltimento dei RAEE contenenti dati personali.

26. Nel caso in cui i responsabili del trattamento dei dati incaricati dello smaltimento di AEE non siano in possesso delle competenze e/o del *know-how* tecnico necessari per la cancellazione dei dati personali in questione, possono affidare tale compito a incaricati del trattamento qualificati (per esempio, centri di assistenza, fabbricanti e distributori di apparecchiature) in base a quanto stabilito dall'articolo 17, paragrafi 2, 3 e 4, della direttiva 95/46/CE. Tali incaricati del trattamento dovranno a loro volta certificare lo svolgimento delle operazioni in questione e/o effettuarle.

27. Alla luce di tali considerazioni, il GEPD giunge alla conclusione che la rifusione della direttiva dovrebbe aggiungere i principi di protezione dei dati alle disposizioni dedicate alla tutela dell'ambiente.

28. Il GEPD raccomanda pertanto al Consiglio e al Parlamento europeo di includere nell'attuale proposta una disposizione specifica che affermi l'applicabilità della direttiva allo smaltimento dei RAEE, fermo restando quanto disposto dalla direttiva 95/46/CE.

III.3. **Reimpiego o riciclaggio dei RAEE e misure di sicurezza**

29. Ove si trovino nella posizione di decidere in maniera autonoma in merito ai dati contenuti nelle AEE, i soggetti incaricati delle operazioni di smaltimento potrebbero essere considerati quali «responsabili del trattamento dei dati» ([18]). Essi devono pertanto adottare procedure interne al fine di evitare inutili operazioni di trattamento di qualsiasi dato personale contenuto nei RAEE, ossia operazioni diverse da quelle strettamente necessarie per verificare l'effettiva eliminazione dei dati in essi contenuti.

30. Inoltre, non devono consentire a soggetti non autorizzati di venire a conoscenza o di trattare i dati contenuti nei RAEE. In particolare, in caso di riciclaggio o reimpiego di supporti di memorizzazione, e quindi di una loro reimmissione in commercio, sussiste un rischio accresciuto di comunicazione o diffusione impropria di dati personali, nonché la necessità di impedire l'accesso non autorizzato a questo genere di dati.

31. Il GEPD pertanto raccomanda che il Consiglio e il Parlamento europeo includano nella proposta attuale una disposizione specifica che vieti l'immissione in commercio di dispositivi usati non precedentemente sottoposti a misure di sicurezza adeguate, in conformità con gli standard tecnici più avanzati (per esempio, sovrascrittura ripetuta con metodo «multi-pass»), per cancellare eventuali dati personali in essi contenuti.

III.4. **Sicurezza e tutela della vita privata garantite fin dalla fase di progettazione**

32. Il nuovo quadro giuridico sui rifiuti elettrici ed elettronici dovrebbe contenere non soltanto una disposizione specifica relativa al più ampio «principio della progettazione ecocompatibile» delle apparecchiature (cfr. l'articolo 4 della proposta in merito alla «Progettazione dei prodotti»), bensì anche, come è già stato precisato in altri pareri del GEPD ([19]), una disposizione riguardante il principio della «Tutela della vita privata fin dalla fase di progettazione» ([20]) o, più esattamente in questo contesto, della «Sicurezza sin dalla progettazione» ([21]). Nei limiti del possibile, la tutela della vita privata e la protezione dei dati dovrebbero essere integrate «di norma» sin dalla fase della progettazione delle apparecchiature elettriche ed elettroniche, al fine di consentire agli utenti di cancellare, usando un mezzo semplice e gratuito, i dati personali che potrebbero essere contenuti nei dispositivi in caso di loro smaltimento ([22]).

([18]) «Il concetto di responsabile del trattamento è […] basato sui fatti, nel senso che è inteso a ripartire le responsabilità nel caso di influenza reale, e quindi basata su un'analisi *effettiva* piuttosto che formale»: cfr. Gruppo di lavoro articolo 29 per la protezione dei dati, WP 169, parere 1/2010 sui concetti di «responsabile del trattamento» e «incaricato del trattamento», adottato il 16 febbraio 2010.

([19]) Cfr., per esempio, *The EDPS and EU Research and Technological Development*, documento orientativo, 28 aprile 2008, pag. 2; parere del GEPD sui sistemi di trasporto intelligenti (GU C 47 del 25.2.2010, pag. 6); parere del GEPD per quanto riguarda la farmacovigilanza (GU C 229 del 23.9.2009, pag. 19).

([20]) A favore di un'ampia applicazione di tale principio, cfr. il Gruppo di lavoro articolo 29 sulla protezione dei dati — Gruppo di lavoro «Polizia e giustizia», *The Future of Privacy*. Contributo congiunto alla consultazione della Commissione europea sul quadro giuridico per il diritto fondamentale alla protezione dei dati personali, WP 168, adottato il 1º dicembre 2009, pagg. 3 e 12; cfr. anche la raccomandazione della Commissione sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza, C(2009) 3200 definitivo, pag. 8.

([21]) Cfr. comunicazione della Commissione, Programma europeo di ricerca e innovazione in materia di sicurezza — Posizione iniziale della Commissione sulle principali constatazioni e raccomandazioni dell'ESRIF, COM(2009) 691 definitivo, pagg. 6 e 14.

([22]) Cfr. anche GEPD, *Opinion of 18 March 2010 on promoting trust in the Information Society by fostering data protection and privacy.*

33. Questo approccio è chiaramente sostenuto dall'articolo 3, paragrafo 3, lettera c), della direttiva 1999/5/CE ([23]) riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione nonché dall'articolo 14, paragrafo 3, della direttiva 2002/58/CE ([24]).

34. Pertanto, i produttori dovrebbero «integrare» elementi di salvaguardia per la sicurezza e la tutela della vita privata tramite soluzioni tecnologiche ([25]). In questo contesto sarebbe bene promuovere e sostenere iniziative mirate a fornire consulenza ai soggetti interessati a cancellare eventuali dati personali contenuti nei RAEE prima del loro smaltimento (compresi i produttori affinché mettano a disposizione software gratuiti adatti allo scopo) ([26]).

IV. **CONCLUSIONI**

35. Alla luce di quanto precede, il GEPD raccomanda che le autorità preposte alla protezione dei dati, in particolare attraverso il Gruppo di lavoro articolo 29, e il GEPD stesso partecipino in stretta collaborazione a iniziative vertenti sullo smaltimento dei RAEE, mediante una consultazione in una fase sufficientemente precoce prima dell'elaborazione di misure pertinenti.

36. Considerando il contesto in cui i dati personali vengono sottoposti a trattamento, il GEPD raccomanda l'inserimento nella proposta di disposizioni specifiche che:

— affermino che la direttiva sui RAEE trova applicazione fermo restando il disposto della direttiva 95/46/CE,

— vietino l'immissione in commercio dei dispositivi usati che non siano stati precedentemente sottoposti a misure di sicurezza adeguate, in conformità con gli standard tecnici più avanzati, al fine di cancellare eventuali dati personali in essi contenuti,

— in merito al principio della «Tutela della vita privata fin dalla fase della progettazione» o della «Sicurezza sin dalla progettazione»: nei limiti del possibile, la tutela della vita privata e la protezione dei dati dovrebbero essere integrate «di norma» sin dalla fase della progettazione delle apparecchiature elettriche ed elettroniche, al fine di consentire agli utenti di cancellare, usando modalità semplici e gratuitamente, i dati personali che potrebbero essere contenuti in dispositivi in caso di smaltimento.

37. Pertanto, il GEPD raccomanda vivamente che, in conformità con la direttiva 95/46/CE, la proposta venga così modificata:

— considerando 11: «Inoltre, la presente direttiva dovrebbe applicarsi fatta salva la normativa in materia di protezione dei dati, in particolare la direttiva 95/46/CE. Poiché per apparecchiature elettriche ed elettroniche (AEE) si intende un'ampia gamma di prodotti che comprende una disparata serie di supporti in grado di contenere dati personali — quali le apparecchiature informatiche e di telecomunicazione (per esempio, personal computer, laptop, terminali per i servizi di comunicazione elettronica) — le operazioni di smaltimento collegate a tali apparecchiature, in particolare il reimpiego e il riciclaggio, possono presentare rischi di accesso non autorizzato ai dati personali contenuti nei RAEE. Pertanto, nei limiti del possibile, sarebbe opportuno includere di norma elementi di salvaguardia per la tutela della vita privata e la protezione dei dati nella progettazione di apparecchiature elettriche ed elettroniche capaci di contenere dati personali per consentire agli utenti di cancellare, agevolmente e senza costi aggiuntivi, eventuali informazioni di questo genere al momento dello smaltimento»,

— articolo 2, paragrafo 3: «La presente direttiva si applica fatta salva la normativa in materia di protezione dei dati, in particolare la direttiva 95/46/CE.»

38. In aggiunta, il GEPD ritiene opportuno che si considerino le seguenti modifiche:

— articolo 4, paragrafo 2: «Gli Stati membri incoraggiano misure volte a favorire la progettazione e la produzione di apparecchiature elettriche ed elettroniche che agevolino la cancellazione di eventuali dati personali contenuti nelle AEE al momento del loro smaltimento»,

— articolo 8, paragrafo 7: «Gli Stati membri assicurano che ogni RAEE raccolto contenente dati personali che sia sottoposto a trattamento ai fini del riciclaggio o del reimpiego non sia reimmesso in commercio a meno che tali dati non siano stati cancellati utilizzando le migliori tecniche disponibili»,

([23]) Articolo 3, paragrafo 3, della direttiva 1999/5/CE del Parlamento europeo e del Consiglio, del 9 marzo 1999, riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità (GU L 91 del 7.4.1999, pag. 10): «[…] la Commissione può stabilire che gli apparecchi all'interno di determinate categorie o determinati tipi di apparecchi siano costruiti in modo da […] contenere elementi di salvaguardia per garantire la protezione dei dati personali e della vita privata dell'utente o dell'abbonato».

([24]) «All'occorrenza, possono essere adottate misure dirette a garantire che le apparecchiature terminali siano costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali in conformità della direttiva 1999/5/CE e della decisione 87/95/CEE del Consiglio, del 22 dicembre 1986, relativa alla normalizzazione nel settore delle tecnologie dell'informazione delle telecomunicazioni». Cfr. anche il considerando 46 della medesima direttiva, menzionato alla nota 13.

([25]) A sostegno di questa prospettiva politica, cfr. anche V. Reding, discorso programmatico in occasione della Giornata della protezione dei dati, 28 gennaio 2010, Parlamento europeo, Bruxelles, SPEECH/10/16: «Le imprese devono sfruttare il proprio potenziale innovativo per migliorare la tutela della vita privata e la protezione dei dati personali fin dall'inizio del ciclo di produzione. Il principio della "tutela della vita privata fin dalla fase di progettazione" è un principio che risponde agli interessi dei cittadini e delle imprese. La tutela della vita privata fin dalla fase di progettazione comporterà un aumento della protezione dei singoli individui, nonché un incremento della fiducia nei nuovi prodotti e servizi, che a sua volta avrà un impatto positivo per l'economia. Ho potuto vedere di persona alcuni esempi incoraggianti, ma c'è ancora molto da fare in tal senso».

([26]) Cfr., per esempio, Royal Canadian Mounted Police, *B2-002 — IT Media Overwrite and Secure Erase Products* (05/2009), in http://www.rcmp-grc.gc.ca/ts-st/pubs/it-ti-sec/index-eng.htm

— articolo 14, paragrafo 6: «Gli Stati membri possono esigere che gli utenti delle AEE contenenti dati personali siano informati da produttori e/o distributori, per esempio nelle istruzioni d'uso o presso i punti vendita, in merito alla necessità di cancellare dati personali che potrebbero essere contenuti nelle AEE prima del loro smaltimento».

Fatto a Bruxelles, il 14 aprile 2010.

Peter HUSTINX

Garante europeo della protezione dei dati

II

(Comunicazioni)

COMUNICAZIONI PROVENIENTI DALLE ISTITUZIONI, DAGLI ORGANI E DAGLI ORGANISMI DELL'UNIONE EUROPEA

COMMISSIONE EUROPEA

Autorizzazione degli aiuti di Stato sulla base degli articoli 107 e 108 del TFUE

Casi contro i quali la Commissione non solleva obiezioni

(Testo rilevante ai fini del SEE, eccetto per i prodotti dell'allegato I del trattato)

(2010/C 280/03)

Data di adozione della decisione	6.7.2010
Numero di riferimento dell'aiuto di Stato	N 42/10
Stato membro	Finlandia
Regione	—
Titolo (e/o nome del beneficiario)	Tuki maataloustuotannon lopettamiseen
Base giuridica	Laki maatalouden harjoittamisesta luopumisen tukemisesta (612/2006), sellaisena kuin se on viimeksi muutettuna lailla (1787/2009); Valtioneuvoston asetus maatalouden harjoittamisesta luopumisen tukemisesta (25/2007)
Tipo di misura	Sostegno al prepensionamento
Obiettivo	Sviluppo settoriale
Forma dell'aiuto	Sovvenzione diretta
Dotazione di bilancio	184 milioni di EUR
Intensità	Variabile
Durata	1.1.2011-31.12.2014
Settore economico	Produzione primaria di prodotti agricoli
Nome e indirizzo dell'autorità che eroga l'aiuto	Maa- ja metsätalousministeriö PL 30 FI-00023 Valtioneuvosto Helsinki SUOMI/FINLAND
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

Data di adozione della decisione	20.7.2010
Numero di riferimento dell'aiuto di Stato	N 131/10
Stato membro	Bulgaria
Regione	—
Titolo (e/o nome del beneficiario)	Държавна помощ за компенсиране на загуби, понесени от селскостопанските производители в напълно опустошени райони вследствие на природни бедствия или неблагоприятни климатични условия (нотификация на изменение)
Base giuridica	Чл. 12, ал. 1, т. 2 и чл. 12, ал. 2, т. 1, буква „а“ от Закона за подпомагане на земеделските производители, ДВ 58/98 Указания за предоставяне на държавна помощ за компенсиране на загуби в следствие на природни бедствия и неблагоприятни климатични условия
Tipo di misura	Regime di aiuti
Obiettivo	Condizioni climatiche avverse, calamità naturali o eventi eccezionali
Forma dell'aiuto	Sovvenzione diretta
Dotazione di bilancio	Bilancio complessivo: 600 BGN (in milioni)
Intensità	80 %
Durata	Fino al 31.12.2013
Settore economico	Settore agricolo
Nome e indirizzo dell'autorità che eroga l'aiuto	Държавен фонд „Земеделие“ Бул. „Цар Борис III“ № 136 1618 София/Sofia БЪЛГАРИЯ/BULGARIA
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

---

Data di adozione della decisione	9.7.2010
Numero di riferimento dell'aiuto di Stato	N 133/10
Stato membro	Italia
Regione	Provincia autonoma di Bolzano
Titolo (e/o nome del beneficiario)	Disciplina degli aiuti regionali in materia di foreste
Base giuridica	Legge Provinciale del 21.10.1996 «Ordinamento Forestale» decreto del Presidente della Giunta provinciale 31 luglio 2000, n. 29 Regolamento all'ordinamento forestale 2000; Programma di sviluppo rurale 2007-2013, misure 111, 122, 123 settore Foreste, 125 Settore Foreste, 226, 227
Tipo di misura	Regime di aiuti
Obiettivo	Sostegno al settore forestale
Forma dell'aiuto	Sovvenzione diretta

Dotazione di bilancio	Importo massimo globale: 30 milioni di EUR
Intensità	Fino a un massimo del 100 % dei costi ammissibili
Durata	2010-2013
Settore economico	Settore forestale
Nome e indirizzo dell'autorità che eroga l'aiuto	Provincia Autonoma di Bolzano Ripartizione Foreste Ufficio economia montana Via Brennero 6 39100 Bolzano BZ ITALIA
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

---

Data di adozione della decisione	4.6.2010
Numero di riferimento dell'aiuto di Stato	N 148/10
Stato membro	Italia
Regione	Provincia autonoma di Trento
Titolo (e/o nome del beneficiario)	Ricostituzione del potenziale forestale e interventi preventivi
Base giuridica	Piano di sviluppo rurale della Provincia autonoma di Trento 2007-2013 (Misura 226)
Tipo di misura	Regime di aiuti
Obiettivo	Aiuti al settore forestale
Forma dell'aiuto	Sovvenzione diretta
Dotazione di bilancio	Stanziamento annuo massimo: 3,25 Mio EUR Importo complessivo massimo: 13 Mio EUR
Intensità	Fino al 100 % delle spese ammissibili
Durata	31.12.2013
Settore economico	Settore forestale
Nome e indirizzo dell'autorità che eroga l'aiuto	Provincia autonoma di Trento Piazza Dante 5 38122 Trento TN ITALIA
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

---

Data di adozione della decisione	17.6.2010
Numero di riferimento dell'aiuto di Stato	N 209/10
Stato membro	Francia
Regione	Dipartimenti Charente-Maritime, Vendée e Gironde
Titolo (e/o nome del beneficiario)	Aides aux exploitants agricoles victimes des inondations marines causées par la tempête Xynthia du 28 février 2010.
Base giuridica	— Articles L 361-1 et s. du code rural (le budget nécessaire aux aides d'État affectées à ce dispositif sera prélevé sur le fonds national de garantie des calamités agricoles). — Articles 1511-2 à 1511-6 du code général des collectivités territoriales et L 3231-2 et suivants pour les aides des collectivités territoriales. — Arrêté interministériel du 1er mars 2010 de reconnaissance de catastrophe naturelle. — Arrêté interministériel du 11 mars 2010 de reconnaissance de catastrophe naturelle.
Tipo di misura	Regime di aiuti
Obiettivo	Indennizzo dei danni subiti dagli agricoltori
Forma dell'aiuto	Sovvenzione diretta
Dotazione di bilancio	Massimo 43 000 000 EUR
Intensità	Massimo 60 %
Durata	4 anni
Settore economico	Agricoltura
Nome e indirizzo dell'autorità che eroga l'aiuto	Ministère de l'alimentation, de l'agriculture et de la pêche 78 rue de Varenne 75349 Paris 07 SP FRANCE
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

Autorizzazione degli aiuti di Stato sulla base degli articoli 107 e 108 del TFUE

Casi contro i quali la Commissione non solleva obiezioni

(Testo rilevante ai fini del SEE, eccetto per i prodotti dell'allegato I del trattato)

(2010/C 280/04)

Data di adozione della decisione	16.7.2010
Numero di riferimento dell'aiuto di Stato	N 414/09
Stato membro	Francia
Regione	—
Titolo (e/o nome del beneficiario)	Aides de l'Agence de l'eau Artois-Picardie aux engagements agro-environnementaux dans le bassin Artois Picardie (EAEAP)
Base giuridica	Loi nº 2006-1772 du 30 décembre 2006 sur l'eau et les milieux aquatiques (JORF nº 303 du 31 décembre 2006). Proposition de dispositif pour des aides agro-environnementales de l'agence de l'eau Artois-Picardie
Tipo di misura	Regime di aiuti
Obiettivo	Aiuti alle misure agroambientali
Forma dell'aiuto	Sovvenzioni dirette
Dotazione di bilancio	Spesa annua: 21,33 Mio EUR Importo complessivo: 64 Mio EUR
Intensità	Massimo 100 % delle spese ammissibili
Durata	2010-2012
Settore economico	Agricoltura
Nome e indirizzo dell'autorità che eroga l'aiuto	Agence de l'eau Artois-Picardie 200 rue Marceline BP 818 59508 Douai FRANCE
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

---

Data di adozione della decisione	3.2.2010
Numero di riferimento dell'aiuto di Stato	N 582/09
Stato membro	Italia
Regione	Sardegna
Titolo (e/o nome del beneficiario)	Ristrutturazione dell'azienda «Cooperativa viticultori della Planargia»

Base giuridica	Legge regionale 19 gennaio 1998, n. 4 «Interventi a favore di aziende agricole in difficoltà» Legge regionale 29 maggio 2007, n. 2 «Legge finanziaria 2007» — articolo 21 Decreto dell'Assessore n. 2532/DecA/105 del 13.10.2009
Tipo di misura	Aiuto individuale
Obiettivo	Ristrutturazione di imprese in difficoltà
Forma dell'aiuto	Sovvenzione diretta
Dotazione di bilancio	294 540 EUR
Intensità	75 %
Durata	Dopo l'approvazione dell'aiuto da parte della Commissione
Settore economico	Agricoltura (settore vitivinicolo)
Nome e indirizzo dell'autorità che eroga l'aiuto	Assessorato dell'agricoltura e riforma agro-pastorale Via Pessagno 4 09126 Cagliari CA ITALIA
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

---

Data di adozione della decisione	20.7.2010
Numero di riferimento dell'aiuto di Stato	NN 26/10
Stato membro	Repubblica ceca
Regione	—
Titolo (e/o nome del beneficiario)	Vrácení části spotřební daně na pohonné hmoty spotřebované při zemědělské produkci (změna režimu podpory č. N 678/07)
Base giuridica	Zákon č. 353/2003 Sb., o spotřebních daních, ve znění pozdějších předpisů Vyhláška 48/2008 Sb. o způsobu výpočtu nároku na vrácení spotřební daně zaplacené v cenách některých minerálních olejů spotřebovaných v zemědělské prvovýrobě
Tipo di misura	Regime di aiuto
Obiettivo	Aiuto connesso a esenzioni fiscali a norma della direttiva 2003/96/CE
Forma dell'aiuto	Agevolazione fiscale
Dotazione di bilancio	Totale: 6 800 Mio CZK (circa 272 Mio EUR) Annuo: 1 700 Mio CZK (circa 68 Mio EUR)
Intensità	60 % delle spese ammissibili
Durata	Fino al 31 dicembre 2013

Settore economico	Agricoltura
Nome e indirizzo dell'autorità che eroga l'aiuto	Ministerstvo zemědělství Těšnov 17 117 05 Praha 1 ČESKÁ REPUBLIKA
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

Data di adozione della decisione	16.7.2010
Numero di riferimento dell'aiuto di Stato	N 213/10
Stato membro	Estonia
Regione	—
Titolo (e/o nome del beneficiario)	Eesti maaelu arengukava 2007–2013 meede 2.7 „Natura 2000 toetus erametsamaale"
Base giuridica	Eesti maaelu arengukava 2007–2013, peatükk 5.3.2.2; Põllumajandusministri 11.3.2010. aasta määrus nr 26 „Natura 2000 alal asuva erametsamaa kohta antava toetuse saamise nõuded, toetuse taotlemise ja taotluse menetlemise täpsem kord"; Euroopa Liidu ühise põllumajanduspoliitika rakendamise seadus.
Tipo di misura	Aiuto a favore del settore forestale
Obiettivo	Silvicoltura
Forma dell'aiuto	Sovvenzione diretta
Dotazione di bilancio	Bilancio complessivo di 326 milioni di EEK (circa 20,8 milioni di EUR)
Intensità	Fino al 100 % dei costi ammissibili.
Durata	A decorrere dalla data della decisione della Commissione fino al 31 dicembre 2013
Settore economico	Silvicoltura
Nome e indirizzo dell'autorità che eroga l'aiuto	Põllumajanduse Registrite ja Informatsiooni Amet Narva 3 51009 Tartu EESTI/ESTONIA
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

Autorizzazione degli aiuti di Stato sulla base degli articoli 107 e 108 del TFUE

Casi contro i quali la Commissione non solleva obiezioni

(Testo rilevante ai fini del SEE, eccetto per i prodotti dell'allegato I del trattato)

(2010/C 280/05)

Data di adozione della decisione	12.8.2010
Numero di riferimento dell'aiuto di Stato	N 83/10
Stato membro	Italia
Regione	Sardegna
Titolo (e/o nome del beneficiario)	Aiuto alla ristrutturazione a favore dell'Unione Pastori Società Cooperativa Agricola, registrata nella Z.I Taccu — Nurri Cagliari
Base giuridica	Legge regionale 19 gennaio 1998 «Interventi a favore delle aziende agricole in difficoltà» Articolo 21 della legge regionale 29 maggio 2007, n. 2 Decreto regionale n. 343/DecA/7 del 4 febbraio 2010
Tipo di misura	Aiuto individuale
Obiettivo	Ristrutturazione di una media impresa
Forma dell'aiuto	Sovvenzione diretta
Dotazione di bilancio	1 Mio di EUR
Intensità	33,3 % dei costi totali di ristrutturazione (3 Mio di EUR)
Durata	Aiuto ad hoc
Settore economico	Agricoltura
Nome e indirizzo dell'autorità che eroga l'aiuto	Regione Autonoma Sardegna Assessorato dell'Agricoltura Via Pessagno 4 09125 Cagliari CA ITALIA
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

Autorizzazione degli aiuti di Stato sulla base degli articoli 107 e 108 del TFUE

Casi contro i quali la Commissione non solleva obiezioni

(Testo rilevante ai fini del SEE, eccetto per i prodotti dell'allegato I del trattato)

(2010/C 280/06)

Data di adozione della decisione	7.4.2010
Numero di riferimento dell'aiuto di Stato	N 716/09
Stato membro	Grecia
Regione	Περιοχές που επλήγησαν από τις πυρκαγιές του 2009
Titolo (e/o nome del beneficiario)	Πρόγραμμα κρατικών οικονομικών ενισχύσεων για την αντιστάθμιση ζημιών από πυρκαγιές έτους 2009
Base giuridica	Σχέδιο ΚΥΑ για τη λήψη μέτρων υπέρ των παραγωγών της χώρας των οποίων οι γεωργοκτηνοτροφικές τους εκμεταλλεύσεις ζημιώθηκαν από πυρκαγιές κατά το έτος 2009
Tipo di misura	Indennizzo per i danni causati agli strumenti di produzione agricola da eventi di carattere eccezionale
Obiettivo	Eventi di carattere eccezionale
Forma dell'aiuto	Sovvenzione diretta
Dotazione di bilancio	Stanziamento complessivo di 8 000 000 EUR
Intensità	I produttori che hanno subito danni pari ad un minimo del 30 % potranno beneficiare dell'aiuto. L'intensità dell'aiuto sarà in funzione della natura dell'oggetto danneggiato ed oscillerà fra il 50 % e l'80 %
Durata	A decorrere dall'approvazione del regime fino al 31 dicembre 2013
Settore economico	Settore agricolo
Nome e indirizzo dell'autorità che eroga l'aiuto	α. Υπουργείο Αγροτικής Ανάπτυξης και Τροφίμων Αχαρνών 2 101 76 Αθήνα/Athens ΕΛΛΑΔΑ/GREECE β. ΕΛΓΑ Μεσογείων 45 115 10 Αθήνα/Athens ΕΛΛΑΔΑ/GREECE
Altre informazioni	—

Il testo delle decisioni nelle lingue facenti fede, ad eccezione dei dati riservati, è disponibile sul sito:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_it.htm

IV

(Informazioni)

INFORMAZIONI PROVENIENTI DALLE ISTITUZIONI, DAGLI ORGANI E DAGLI ORGANISMI DELL'UNIONE EUROPEA

COMMISSIONE EUROPEA

Tassi di cambio dell'euro [1]

15 ottobre 2010

(2010/C 280/07)

1 euro =

	Moneta	Tasso di cambio		Moneta	Tasso di cambio
USD	dollari USA	1,4089	AUD	dollari australiani	1,4142
JPY	yen giapponesi	114,28	CAD	dollari canadesi	1,4165
DKK	corone danesi	7,4564	HKD	dollari di Hong Kong	10,9300
GBP	sterline inglesi	0,87750	NZD	dollari neozelandesi	1,8565
SEK	corone svedesi	9,2230	SGD	dollari di Singapore	1,8244
CHF	franchi svizzeri	1,3423	KRW	won sudcoreani	1 564,64
ISK	corone islandesi		ZAR	rand sudafricani	9,5833
NOK	corone norvegesi	8,0925	CNY	renminbi Yuan cinese	9,3568
BGN	lev bulgari	1,9558	HRK	kuna croata	7,3355
CZK	corone ceche	24,515	IDR	rupia indonesiana	12 530,82
EEK	corone estoni	15,6466	MYR	ringgit malese	4,3443
HUF	fiorini ungheresi	274,18	PHP	peso filippino	60,847
LTL	litas lituani	3,4528	RUB	rublo russo	42,5650
LVL	lats lettoni	0,7097	THB	baht thailandese	42,015
PLN	zloty polacchi	3,9050	BRL	real brasiliano	2,3369
RON	leu rumeni	4,2765	MXN	peso messicano	17,4580
TRY	lire turche	1,9808	INR	rupia indiana	62,1320

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

DECISIONE DELLA COMMISSIONE

del 14 ottobre 2010

che istituisce un gruppo di alto livello sulla competitività e la crescita sostenibile dell'industria automobilistica nell'Unione europea (già gruppo «CARS 21»)

(2010/C 280/08)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

considerando quanto segue:

(1) L'articolo 173 del trattato assegna all'Unione europea e agli Stati membri il compito di assicurare le condizioni necessarie alla competitività dell'industria dell'Unione. Secondo l'articolo 191 del trattato, la politica dell'Unione in materia ambientale contribuisce a promuovere misure destinate a salvaguardare, tutelare e migliorare la qualità dell'ambiente e a combattere i cambiamenti climatici.

(2) Nel quadro della politica industriale della Commissione, il processo «CARS 21» («Competitive Automotive Regulatory System for the 21st century»), che ha avuto inizio nel 2005, ha formulato raccomandazioni per un'azione a breve, medio e lungo termine che, nel quadro normativo per l'industria automobilistica europea, rafforzi la competitività globale, accresca l'occupazione e favorisca nuovi progressi sul piano della sicurezza e della tutela dell'ambiente a costi accettabili per i consumatori.

(3) Nella sua comunicazione «EUROPA 2020 — Una strategia per una crescita intelligente, sostenibile e inclusiva» ([1]), la Commissione presenta proposte per modernizzare e «decarbonizzare» il settore dei trasporti e promuovere nuove tecnologie, comprese le automobili elettriche. L'iniziativa faro «Una politica industriale per l'era della globalizzazione» intende dar vita a una politica industriale che crei le condizioni migliori per mantenere e sviluppare in Europa una base industriale solida, competitiva e diversificata, e promuova la sostenibilità favorendo un uso più efficace dell'energia e delle risorse da parte delle industrie manifatturiere. L'iniziativa faro «Un'Europa efficiente sotto il profilo delle risorse» promuoverà misure infrastrutturali di ampia portata come la creazione di infrastrutture di rete per la mobilità elettrica, la gestione intelligente del traffico e soprattutto le nuove tecnologie, comprese quelle delle automobili elettriche e ibride.

(4) La comunicazione della Commissione «Una strategia europea per i veicoli puliti ed efficienti sul piano energetico» ([2]) definisce obiettivi a breve e a lungo termine per sostenere la ricerca e l'innovazione, trovare soluzioni per la produzione e la distribuzione dell'energia elettrica, stimolare l'occupazione e indurre i consumatori ad acquistare veicoli verdi.

(5) È perciò necessario costituire un gruppo di esperti nel campo della competitività e della crescita sostenibile dell'industria automobilistica europea, che riprenda il processo «CARS 21», e definirne i compiti e la struttura.

(6) Il gruppo deve contribuire a definire politiche e misure, da attuare a livello dell'Unione europea, a livello nazionale e con l'intervento di altre parti interessate, che favoriscano la competitività e la crescita sostenibile dell'industria automobilistica europea.

(7) Il gruppo deve essere costituito da rappresentanti del Parlamento europeo, della Commissione, degli Stati membri e delle parti interessate dell'industria e della società civile, in particolare da rappresentanti dei consumatori, delle organizzazioni sindacali e delle organizzazioni non governative.

(8) La diffusione delle informazioni da parte dei membri del gruppo deve essere regolamentata, nel rispetto delle disposizioni della Commissione in materia di sicurezza riportate nell'allegato della decisione 2001/844/CE, CECA, Euratom della Commissione, del 29 novembre 2001, che modifica il regolamento interno della Commissione ([3]).

(9) Il trattamento dei dati personali deve essere conforme alle disposizioni del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati ([4]).

(10) È opportuno stabilire un periodo di applicazione della presente decisione. La Commissione valuterà a tempo debito l'opportunità di una proroga,

DECIDE:

Articolo 1

Gruppo

È istituito un gruppo di alto livello sulla competitività e la crescita sostenibile dell'industria automobilistica nell'Unione europea (di seguito «il gruppo») già esistente informalmente con la denominazione «CARS 21» («Competitive Automotive Regulatory System for the 21st century»).

([1]) COM(2010) 2020.
([2]) COM(2010) 186.
([3]) GU L 317 del 3.12.2001, pag. 1.
([4]) GU L 8 del 12.1.2001, pag. 1.

Articolo 2

Compiti

Il gruppo ha il compito di:

1) assistere la Commissione nelle questioni relative alla competitività e alla crescita sostenibile dell'industria automobilistica;

2) svolgere un'analisi economica e statistica dei fattori che determinano i cambiamenti strutturali nell'industria automobilistica e di altri fattori che influiscono sulla competitività dell'industria automobilistica dell'Unione europea;

3) assistere la Commissione nella messa in atto della politica definita dalla strategia «EUROPA 2020», delle iniziative faro «Un'Europa efficiente sotto il profilo delle risorse» e «Una politica industriale per l'era della globalizzazione» e della comunicazione COM(2010) 186 «Una strategia europea per i veicoli puliti ed efficienti sul piano energetico», con l'obiettivo di mantenere nell'Unione europea un'industria automobilistica competitiva e sostenibile;

4) contribuire a una transizione economica e sociale senza scosse ed equilibrata con una gestione previdente dei processi di ristrutturazione e del fabbisogno di competenze e di corrispondenti qualifiche, tenendo conto dei risultati del «Partenariato europeo per l'anticipazione dei cambiamenti nel settore dell'automobile»;

5) formulare una serie di raccomandazioni riguardanti in modo specifico il settore dell'automobile, dirette alle autorità dell'Unione europea e degli Stati membri, all'industria e alle organizzazioni della società civile;

6) definire principi di buona condotta per promuovere la trasparenza nelle relazioni commerciali e contrattuali tra le parti di accordi verticali nel settore dei veicoli a motore;

7) prestare la sua consulenza su aspetti specifici dell'attuazione della strategia «EUROPA 2020» della Commissione per una crescita intelligente, sostenibile e inclusiva.

Articolo 3

Composizione — Nomina

1. Il gruppo è composto da 40 membri.

2. I membri sono nominati a titolo personale. Ogni membro designa un proprio rappresentante personale in un sottogruppo preparatorio permanente (di seguito «sottogruppo preparatorio»).

3. La Commissione nomina i membri del gruppo scegliendoli tra personalità di alto livello che abbiano competenze e responsabilità in ambiti attinenti alla competitività e alla crescita sostenibile dell'industria automobilistica europea. Nel gruppo sono rappresentate in modo equilibrato le varie parti interessate. Il gruppo è costituito da rappresentanti del Parlamento europeo, della Commissione, degli Stati membri, degli attori della catena del valore dell'industria, delle organizzazioni sindacali e della società civile (organizzazioni non governative e dei consumatori).

4. I membri sono nominati per due anni e restano in carica finché non sono sostituiti o il loro mandato giunge al termine. Il mandato può essere rinnovato.

5. I membri che non sono più in grado di contribuire efficacemente ai lavori del gruppo, che si dimettono o non soddisfano le condizioni di cui all'articolo 339 del trattato possono essere sostituiti per il restante periodo del mandato.

6. I nomi dei membri nominati a titolo personale sono pubblicati nel registro dei gruppi di esperti e altre entità simili della Commissione (di seguito «il registro»).

7. I dati personali sono raccolti, trattati e pubblicati in conformità al regolamento (CE) n. 45/2001.

Articolo 4

Funzionamento

1. Il gruppo è presieduto da un rappresentante della Commissione.

2. Il sottogruppo preparatorio prepara le discussioni, i documenti di posizione e i pareri per le azioni e le misure che dovranno essere raccomandate dal gruppo. A tale scopo, opera in stretto contatto con i servizi competenti della Commissione.

3. Il gruppo può, di concerto con i servizi della Commissione, costituire, oltre al sottogruppo preparatorio, gruppi di lavoro incaricati di esaminare questioni specifiche relative ai compiti del gruppo sulla base di un mandato definito dal gruppo. I gruppi di lavoro sono sciolti non appena hanno portato a termine il loro mandato.

4. Il rappresentante della Commissione può invitare a partecipare ai lavori del gruppo, del sottogruppo o dei gruppi di lavoro, in funzione di specifiche esigenze, esperti od osservatori esterni al gruppo in possesso di particolari competenze in una materia all'ordine del giorno. Inoltre, il rappresentante della Commissione può concedere lo status di osservatore a persone, organizzazioni come definite nelle regole orizzontali per i gruppi di esperti (regola 8, paragrafo 3), agenzie dell'UE e paesi candidati all'adesione.

5. I membri dei gruppi di esperti e i loro rappresentanti, così come gli esperti e gli osservatori invitati, sono tenuti al rispetto degli obblighi del segreto professionale stabiliti dai trattati e dalle relative norme di attuazione, nonché delle disposizioni della Commissione in materia di sicurezza riguardanti la protezione delle informazioni classificate UE, riportate nell'allegato della decisione 2001/844/CE, CECA, Euratom della Commissione. In caso di inosservanza di tali obblighi, la Commissione può prendere tutti i provvedimenti giudicati idonei.

6. Le informazioni ottenute nel quadro della partecipazione alle deliberazioni o ai lavori del gruppo, dei sottogruppi o dei gruppi ad hoc non sono divulgate se la Commissione ritiene che riguardino questioni riservate.

7. Le riunioni del gruppo, del sottogruppo preparatorio e dei gruppi di lavoro si svolgono presso le sedi della Commissione. La Commissione assicura i servizi di segreteria. Altri funzionari della Commissione interessati ai lavori possono assistere alle riunioni del gruppo, del sottogruppo preparatorio e dei gruppi di lavoro.

8. Il gruppo adotta il proprio regolamento interno sulla base del regolamento interno adottato dalla Commissione [1].

9. La Commissione pubblica informazioni sulle attività svolte dal gruppo nel registro, o riportando nel registro stesso un *link* verso il sito web corrispondente. La relazione finale è pubblicata non appena possibile dopo l'ultima riunione del gruppo.

Articolo 5

Spese per le riunioni

1. I partecipanti alle attività del gruppo non sono remunerati per i servizi che prestano.

2. La Commissione rimborsa le spese di viaggio e di soggiorno sostenute dai partecipanti alle attività del gruppo in base alle proprie disposizioni interne.

3. Le spese sono rimborsate nei limiti degli stanziamenti disponibili assegnati nel quadro della procedura annuale di assegnazione delle risorse.

Articolo 6

Applicabilità

La presente decisione si applica fino al 14 ottobre 2012.

Fatto a Bruxelles, il 14 ottobre 2010.

Per la Commissione
Antonio TAJANI
Vicepresidente

[1] GU L 55/61 del 5.3.2010, pag. 61.

V

(Avvisi)

PROCEDIMENTI RELATIVI ALL'ATTUAZIONE DELLA POLITICA DELLA CONCORRENZA

COMMISSIONE EUROPEA

Notifica preventiva di una concentrazione

(Caso COMP/M.5927 — BASF/Cognis)

(Testo rilevante ai fini del SEE)

(2010/C 280/09)

1. In data 8 ottobre 2010 è pervenuta alla Commissione la notifica di un progetto di concentrazione in conformità dell'articolo 4 del regolamento (CE) n. 139/2004 del Consiglio [1]. Con tale operazione l'impresa BASF SE («BASF», Germania) acquisisce, ai sensi dell'articolo 3, paragrafo 1, lettera b), del regolamento comunitario sulle concentrazioni, il controllo esclusivo dell'impresa Cognis GmbH («Cognis», Germania) mediante acquisto di quote.

2. Le attività svolte dalle imprese interessate sono le seguenti:

— BASF: prodotti chimici, materie plastiche, prodotti di nobilitazione, soluzioni funzionali e per l'agricoltura, petrolio e gas,

— Cognis: specialità chimiche e ingredienti nutrizionali.

3. A seguito di un esame preliminare, la Commissione ritiene che la concentrazione notificata possa rientrare nel campo d'applicazione del regolamento comunitario sulle concentrazioni. Tuttavia, si riserva la decisione finale al riguardo.

4. La Commissione invita i terzi interessati a presentare eventuali osservazioni sulla concentrazione proposta.

Le osservazioni devono pervenire alla Commissione entro dieci giorni dalla data di pubblicazione della presente comunicazione. Le osservazioni possono essere trasmesse alla Commissione per fax (+32 22964301), per e-mail all'indirizzo COMP-MERGER-REGISTRY@ec.europa.eu o per posta, indicando il riferimento COMP/M.5927 — BASF/Cognis, al seguente indirizzo:

Commissione europea
Direzione generale della Concorrenza
Protocollo Concentrazioni
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

[1] GU L 24 del 29.1.2004, pag. 1 («il regolamento comunitario sulle concentrazioni»).

Notifica preventiva di una concentrazione

(Caso COMP/M.5982 — CVCII/Advance Properties/Huvepharma)

Caso ammissibile alla procedura semplificata

(Testo rilevante ai fini del SEE)

(2010/C 280/10)

1. In data 8 ottobre 2010 è pervenuta alla Commissione la notifica di un progetto di concentrazione in conformità dell'articolo 4 e a seguito di un rinvio ai sensi dell'articolo 4, paragrafo 5, del regolamento (CE) n. 139/2004 del Consiglio ([1]). Con tale operazione le imprese Citigroup Venture Capital International Investment G.P. Limited («CVCII», Jersey), controllata da Citigroup, Inc. (USA), e Advance Properties OOD («Advance Properties», Bulgaria) acquisiscono, ai sensi dell'articolo 3, paragrafo 1, lettera b), del regolamento comunitario sulle concentrazioni, il controllo comune di Huvepharma AD («Huvepharma», Bulgaria), attualmente sotto il controllo esclusivo di Advance Properties, mediante acquisto di quote.

2. Le attività svolte dalle imprese interessate sono le seguenti:

— Citigroup: prestazione di servizi finanziari tra cui servizi bancari, intermediazione e gestione di fondi di private equity,

— Advance Properties: investimenti nei settori farmaceutico, immobiliare, dell'energia e della navigazione,

— Huvepharma: produzione di prodotti farmaceutici, prevalentemente nutrizionali e ad uso veterinario.

3. A seguito di un esame preliminare la Commissione ritiene che la concentrazione notificata possa rientrare nel campo d'applicazione del regolamento comunitario sulle concentrazioni. Tuttavia, si riserva la decisione definitiva al riguardo. Si rileva che, ai sensi della comunicazione della Commissione concernente una procedura semplificata per l'esame di determinate concentrazioni a norma del regolamento comunitario sulle concentrazioni ([2]), il presente caso potrebbe soddisfare le condizioni per l'applicazione della procedura di cui alla comunicazione stessa.

4. La Commissione invita i terzi interessati a presentare eventuali osservazioni sulla concentrazione proposta.

Le osservazioni devono pervenire alla Commissione entro dieci giorni dalla data di pubblicazione della presente comunicazione. Le osservazioni possono essere trasmesse alla Commissione per fax (+32 22964301), per e-mail all'indirizzo COMP-MERGER-REGISTRY@ec.europa.eu o per posta, indicando il riferimento COMP/M.5982 — CVCII/Advance Properties/Huvepharma, al seguente indirizzo:

Commissione europea
Direzione generale della Concorrenza
Protocollo Concentrazioni
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

([1]) GU L 24 del 29.1.2004, pag. 1 («il regolamento comunitario sulle concentrazioni»).
([2]) GU C 56 del 5.3.2005, pag. 32 («la comunicazione sulla procedura semplificata»).

Avviso del ministro degli Affari economici del Regno dei Paesi Bassi a norma dell'articolo 3, paragrafo 2, della direttiva 94/22/CE del Parlamento europeo e del Consiglio, relativa alle condizioni di rilascio e di esercizio delle autorizzazioni alla prospezione, ricerca e coltivazione di idrocarburi

(2010/C 280/11)

Il ministro degli Affari economici rende noto che è pervenuta una domanda di autorizzazione alla prospezione di idrocarburi per una parte del settore P18, denominata P18b, come appare sulla mappa contenuta nell'allegato 3 del regolamento sulle attività estrattive (Mijnbouwregeling, Stcrt. 2002, n. 245).

Vista la direttiva summenzionata e considerato l'articolo 15 della Mijnbouwwet (legge sulle attività estrattive, Stb. 2002, n. 542), il ministro degli Affari economici indice un invito a presentare candidature in concorrenza per un'autorizzazione alla prospezione di idrocarburi per il sottosettore P18b della piattaforma continentale dei Paesi Bassi.

Il sottosettore P18b è delimitato dagli archi di parallelo che collegano le coppie di punti A-B e H-I, dagli archi di meridiano che collegano le coppie di punti B-C, G-H e A-I, dai circoli massimi che collegano le coppie di punti C-D e E-F, dall'arco di circolo 1 tra i punti D e E e dall'arco di circolo 2 tra i punti F e G.

Le coordinate dei punti summenzionati sono le seguenti:

Punto	°	′	″ Long. E	°	′	″ Lat. N
A	3	40	0,000	52	10	0,000
B	3	47	0,000	52	10	0,000
C	3	47	0,000	52	4	21,072
D	3	47	16,385	52	4	16,801
E	3	51	32,620	52	6	15,485
F	3	51	40,829	52	6	37,449
G	4	0	0,000	52	4	48,172
H	4	0	0,000	52	0	0,000
I	3	40	0,000	52	0	0,000

L'arco di circolo 1 ha il centro a 3° 54′ 0,000″ Long. E, 52° 1′ 30,000″ Lat. N e un raggio di 5 miglia marine.

L'arco di circolo 2 ha il centro a 3° 53′ 34,000″ Long. E, 52° 1′ 46,000″ Lat. N e un raggio di 5 miglia marine.

La posizione dei punti summenzionati è espressa in coordinate geografiche calcolate secondo il sistema europeo di riferimento terrestre.

La superficie del sottosettore P18b misura 313,2 km^2.

L'autorità competente per la concessione dell'autorizzazione è il ministro degli Affari economici. I criteri, le condizioni e i requisiti di cui all'articolo 5, paragrafi 1 e 2, e all'articolo 6, paragrafo 2, della direttiva summenzionata sono stabiliti nella legge sulle attività estrattive (Mijnbouwwet, Stb. 2002, n. 542).

Il termine per la presentazione delle candidature è di 13 settimane dalla pubblicazione del presente invito nella *Gazzetta ufficiale dell'Unione europea*. Le candidature devono essere inviate al seguente indirizzo:

De Minister van Economische Zaken
ter attentie van J. C. De Groot, directeur Energiemarkt
ALP/562
Bezuidenhoutseweg 30
Postbus 20101
2500 EJ Den Haag
NEDERLAND

Le candidature presentate dopo la scadenza del termine suddetto non saranno prese in considerazione.

La decisione in merito alle candidature sarà presa entro 12 mesi dalla scadenza del termine di cui sopra.

Per ulteriori informazioni contattare il signor E. J. Hoppel al seguente numero di telefono: +31 703797088.

RETTIFICHE

Rettifica della pubblicazione della domanda di riconoscimento di una menzione tradizionale ai sensi dell'articolo 33 del regolamento (CE) n. 607/2009 della Commissione

(Gazzetta ufficiale dell'Unione europea C 275 del 12 ottobre 2010)

(2010/C 280/12)

Alle pagine 11, 13 e 15, la frase «autorità competente dello Stato membro:» deve essere soppressa.

Rettifiche

IT

PREZZO DEGLI ABBONAMENTI 2010 (IVA esclusa, spese di spedizione ordinaria incluse)

Gazzetta ufficiale dell'UE, serie L + C, unicamente edizione su carta	22 lingue ufficiali dell'UE	1 100 EUR all'anno
Gazzetta ufficiale dell'UE, serie L + C, su carta + CD-ROM annuale	22 lingue ufficiali dell'UE	1 200 EUR all'anno
Gazzetta ufficiale dell'UE, serie L, unicamente edizione su carta	22 lingue ufficiali dell'UE	770 EUR all'anno
Gazzetta ufficiale dell'UE, serie L + C, CD-ROM mensile (cumulativo)	22 lingue ufficiali dell'UE	400 EUR all'anno
Supplemento della Gazzetta ufficiale (serie S — Appalti pubblici), CD-ROM, 2 edizioni la settimana	multilingue: 23 lingue ufficiali dell'UE	300 EUR all'anno
Gazzetta ufficiale dell'UE, serie C — Concorsi	lingua/e del concorso	50 EUR all'anno

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

Ogni versione linguistica è oggetto di un abbonamento separato.

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

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

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

Il formato CD-ROM sarà sostituito dal formato DVD nel 2010.

Vendita e abbonamenti

Gli abbonamenti ai diversi periodici a pagamento, come l'abbonamento alla *Gazzetta ufficiale dell'Unione europea*, sono disponibili presso i nostri distributori commerciali. L'elenco dei distributori commerciali è pubblicato al seguente indirizzo:

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

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

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

Ufficio delle pubblicazioni dell'Unione europea
2985 Lussemburgo
LUSSEMBURGO

IT