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