I

(Risoluzioni, raccomandazioni e pareri)

PARERI

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

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

(2008/C 101/01)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 286,

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

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

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

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 15 marzo 2007 la Commissione ha adottato una comunicazione sull'identificazione a radiofrequenza (RFID) in Europa: verso un quadro politico [1] (di seguito «la comunicazione»). A norma dell'articolo 41 del regolamento (CE) n. 45/2001, il GEPD ha il compito di fornire consulenza alle istituzioni e agli organismi comunitari su tutte le questioni concernenti il trattamento dei dati personali. In conformità di detto articolo, il GEPD presenta il presente parere.

2. Il presente parere deve essere considerato una reazione del GEPD alla comunicazione, nonché ad altre azioni nel settore della RFID che hanno avuto luogo dall'adozione della comunicazione. Sono di seguito riportate altre azioni rilevanti prese in considerazione nel presente parere:

— la decisione della Commissione, del 28 giugno 2007, che istituisce un gruppo di esperti sull'identificazione a radio frequenza (RFID) [2], una conseguenza diretta della comunicazione. Questo gruppo è noto anche come Gruppo delle parti interessate alla RFID. In conformità dell'articolo 4, paragrafo 4, lettera b), della decisione, il GEPD partecipa alle attività del gruppo in qualità di osservatore,

— la risoluzione del Consiglio, del 22 marzo 2007, su una strategia per una società dell'informazione sicura in Europa [3],

— il progetto «RFID e gestione dell'identità» avviato dal Parlamento europeo [4],

[1] COM(2007) 96 defin.
[2] Decisione n. 467/2007/CE (GU L 176 del 6.7.2007, pag. 25).
[3] GU C 68 del 24.3.2007, pag. 1.
[4] Progetto «RFID and identity management — Case studies from the frontline of the development towards ambient intelligence», commissionato dal servizio di valutazione delle scelte scientifiche e tecnologiche (STOA) del Parlamento europeo ed effettuato dall'ETAG (Gruppo europeo per la valutazione tecnologica), http://www.europarl.europa.eu/stoa/default_en.htm

— l'adozione, nel giugno 2007, da parte del Gruppo di lavoro «Articolo 29» per la protezione dei dati del parere n. 4/2007 sul concetto di dati personali ([1]),

— la 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 ([2]), e il parere del GEPD su tale comunicazione del 25 luglio 2007 ([3]),

— l'adozione da parte della Commissione di una proposta di direttiva che modifica (fra l'altro) la direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche ([4]).

3. Il GEPD si compiace della comunicazione della Commissione sulla RFID in quanto affronta le principali questioni che sorgono nel contesto della diffusione della tecnologia RFID senza trascurare quelle determinanti relative alla tutela della vita privata e alla protezione dei dati. Questa comunicazione ha tratto vantaggio da coerenti e rigorosi lavori preparatori. Infatti, essa è stata preceduta da cinque seminari tematici e da una consultazione pubblica on line ([5]) commissionati dalla Commissione.

4. Il GEPD concorda con l'opinione secondo cui i sistemi RFID potrebbero svolgere un ruolo fondamentale in quello sviluppo della società dell'informazione noto come l'«Internet degli oggetti» e condivide pienamente le preoccupazioni espresse al punto 3.2 della stessa comunicazione secondo cui i sistemi RFID possono minacciare la vita privata delle persone e i diritti in materia di protezione dei dati. Infatti, nella relazione annuale 2005, il GEPD ha individuato nella RFID, unitamente alla biometria, agli ambienti di intelligenza diffusa e ai sistemi di gestione dell'identità, sviluppi tecnologici che si prevede avranno un notevole impatto sulla protezione dei dati.

5. Secondo il GEPD, la domesticizzazione delle tecnologie RFID e la loro vasta accettazione non solo saranno raggiunte grazie alla loro allettante convenienza o ai nuovi servizi offerti, ma saranno anche agevolate dai vantaggi di garanzie specifiche e coerenti in materia di protezione dei dati.

6. In breve: il GEPD qualifica la RFID uno sviluppo tecnologico fondamentalmente nuovo, giustamente citato nella comunicazione della Commissione come porta d'ingresso verso una nuova fase di sviluppo della società dell'informazione.

7. Questo sviluppo solleva importanti questioni in differenti settori, tra cui la protezione dei dati e la tutela della vita privata. Il presente parere del GEPD si limita a questo settore.

II. PUNTO CENTRALE DEL PARERE

8. Il presente parere è incentrato in particolare sulle possibili conseguenze di questi sviluppi per la protezione dei dati e la tutela della vita privata. Dette conseguenze sono per il momento incerte, anche per il fatto che lo sviluppo dei sistemi RFID e la loro domesticizzazione sono ancora in corso e non è per nulla chiaro l'esito di questi sviluppi.

9. In tale prospettiva il GEPD adotta l'approccio seguente:

— in primo luogo, è necessario precisare le conseguenze pratiche della diffusione dei sistemi RFID per la protezione dei dati e la tutela della vita privata,

— in secondo luogo, è necessario specificare dette conseguenze, nel contesto del quadro normativo esistente per la protezione dei dati e la tutela della vita privata,

— in terzo luogo, il GEPD affronta la questione se tali conseguenze richiedano o meno norme più specifiche per far fronte alle questioni relative alla protezione dei dati sollevate dall'utilizzo delle tecnologie RFID. Tale questione era stata già segnalata dal GEPD nel suo parere sulla comunicazione relativa alla direttiva sulla protezione dei dati e sarà ulteriormente elaborata nel presente parere.

10. Adottando tale approccio, il GEPD intende promuovere che lo sviluppo dei sistemi RFID e la loro domesticizzazione tenga conto di preoccupazioni giustificate in materia di protezione dei dati e di tutela della vita privata.

III. SPIEGAZIONE DELLE CONSEGUENZE

Sistemi ed etichette RFID

11. Nonostante il fatto che — come già detto — gli sviluppi siano ancora in corso e i risultati siano incerti, è certamente possibile descrivere le principali caratteristiche di questi sviluppi ai fini delle loro conseguenze per la protezione dei dati.

([1]) Documento WP 136, pubblicato nel sito web del Gruppo.
([2]) Comunicazione del 7 marzo 2007 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, COM(2007) 87 defin.
([3]) GU C 255 del 27.10.2007, pag. 1. In appresso: «Parere sulla comunicazione relativa alla direttiva sulla protezione dei dati».
([4]) Proposta, del 13 novembre 2007, di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, il regolamento (CE) n. 2006/2004 sulla cooperazione per la tutela dei consumatori [COM(2007) 698 defin.]. La direttiva 2002/58/CE sarà chiamata «direttiva relativa alla vita privata e alle comunicazioni elettroniche».
([5]) http://www.rfidconsultation.eu/

12. Nel valutare i potenziali aspetti della tecnologia RFID per la protezione dei dati e la tutela della vita privata, è assai importante considerare non solo le etichette RFID separatamente, ma anche l'infrastruttura globale RFID: l'etichetta, il lettore, la rete, la base di dati di riferimento e la base di dati dove sono conservati i dati risultanti dall'associazione etichetta/lettore. Come brevemente sottolineato nell'introduzione della Commissione, i dispositivi RFID non sono semplici «etichette elettroniche» e pertanto le questioni relative alla protezione dei dati non saranno limitate esclusivamente alle etichette, ma saranno estese a tutte le parti dell'infrastruttura globale RFID. Infatti, ciascuno di questi elementi svolge, all'occorrenza, un ruolo nel contribuire all'attuazione del quadro normativo europeo in materia di protezione dei dati. Questi saranno alimentati dalle principali tendenze nell'ambito della società dell'informazione in evoluzione, come una larghezza di banda quasi illimitata, connessioni di rete ubique e una capacità di memorizzazione infinita.

Impatto dei sistemi e delle etichette RFID

13. Nonostante l'esigenza di un approccio più vasto come evidenziato al punto precedente, vari motivi giustificano il fatto di concentrarsi in primo luogo sull'utilizzo della RFID nell'etichettatura dei singoli articoli (*item level tagging* — ILT) di prodotti di consumo come il settore del commercio al dettaglio. Risulta ovvio l'aumento previsto dell'utilizzo, che sembra tendere verso un'estesa applicazione. In contrapposizione ad altre applicazioni RFID di utilizzo ristretto o limitato, l'etichettatura dei singoli articoli offre la potenzialità di diventare un'applicazione da mercato di massa. Sin da ora molti prodotti di consumo sono muniti di un'etichetta RFID. A ciò si ricollega il fatto che tale utilizzo interesserà un numero enorme di individui i cui dati personali saranno probabilmente trattati ogni qualvolta essi acquistano un prodotto in cui sia incorporata un'etichetta RFID.

14. Dovrebbe essere prestata un'attenzione specifica alle conseguenze dell'etichettatura RFID per i proprietari degli articoli. I sistemi RFID potrebbero estendere la relazione tra un articolo e il relativo proprietario. Una volta estesa questa relazione, il proprietario può essere sottoposto a scansione e classificato «di limitata portata finanziaria» o «bersaglio attraente» per le transazioni future; un'eccessiva attribuzione differenziata ([1]) potrebbe comportare una «sanzione» automatica di taluni comportamenti (obbligo di riciclaggio, rifiuti, ecc.). Gli individui non dovrebbero essere soggetti al processo di decisioni automatizzate contrarie. Catalizzato da questa capacità della RFID, aumenta il rischio che la società dell'informazione si avvicini a una situazione in cui saranno prese decisioni automatizzate e in cui si avrà un abuso di tecnologia al fine di regolamentare il comportamento umano.

15. I dati memorizzati o conservati tramite un'etichetta RFID, possono essere dati personali quali definiti all'articolo 2 della direttiva sulla protezione dei dati. Per esempio, le smartcard utilizzate nei viaggi possono contenere informazioni sull'identificazione nonché sui recenti viaggi effettuati dal titolare. Se un individuo senza scrupoli volesse rintracciare delle persone, sarebbe sufficiente collocare in modo strategico dei lettori che forniscano informazioni sugli spostamenti dei titolari della carta, violandone pertanto la vita privata e le informazioni personali.

16. Minacce analoghe alla vita privata potrebbero verificarsi anche se le informazioni memorizzate nell'etichetta RFID non contenessero i nomi delle persone. Le etichette RFID contengono identificatori univoci attribuiti ai prodotti di consumo: se ciascuna etichetta ha un identificatore univoco, tale identificazione può essere utilizzata a fini di sorveglianza. Per esempio, se qualcuno indossa un orologio dotato di etichetta RFID contenente un numero di identificazione, questo potrebbe fungere anche da identificatore univoco per chi indossa l'orologio, benché la sua identità non sia nota. A seconda del modo in cui le informazioni sono utilizzate — e messe in relazione con l'orologio stesso o la persona — la direttiva potrebbe essere applicata o meno. Potrebbe applicarsi, per esempio, qualora siano generate informazioni sui luoghi frequentati dalla persona che saranno probabilmente utilizzate per controllarne il comportamento oppure, per esempio, per la differenziazione dei prezzi, per negare l'accesso o per l'esposizione involontaria alla divulgazione.

17. In tale contesto, è necessario garantire che le applicazioni RFID siano installate con le necessarie misure tecniche per rendere minimo il rischio di divulgazione involontaria di informazioni. Tali misure possono includere il requisito di progettare l'infrastruttura RFID, in particolare le etichette RFID, in modo da impedire questo risultato. Per esempio, le etichette RFID possono essere installate con un «comando kill» che ne consente la disattivazione. Questa opzione sarà ulteriormente discussa al capo IV del presente parere.

18. Offrendo la possibilità di rintracciare i prodotti dopo il punto di vendita, i sistemi RFID introducono nuove questioni nel dibattito sulla vita privata. Infatti due elementi dovranno essere presi in considerazione nell'analisi del loro impatto: fino a che punto l'articolo è considerato personale, e la mobilità dell'articolo ([2]).

19. Il ciclo di vita di un oggetto potrebbe inoltre integrare la necessaria analisi dei rischi e contribuire alla valutazione quantitativa delle potenziali minacce in relazione alla vita privata. Considerato il fatto che un'etichetta non può essere disattivata, il prodotto per l'utente finale con un lungo ciclo di vita sarà in grado di raccogliere più dati pertinenti dal proprietario del prodotto e costruire un profilo più accurato. D'altro canto, il breve ciclo di vita di un articolo come una lattina di bibita dalla produzione fino alla fase di riciclaggio potrebbe presentare rischi minori ed esigere pertanto misure meno rigide di un prodotto con un ciclo di vita di gran lunga superiore.

([1]) Dr.ssa Sarah Spiekermann, direttore del Centro di ricerca sull'economia di Internet di Berlino, seminario sull'RFID e sul calcolo ubiquo organizzato dal Dialogo transatlantico dei consumatori, 13 marzo 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman e Norman G. Einspruch, «Chips, tags and scanners: Ethical challenges for radio frequency identification, Ethics and Information Technology», volume 9, n. 2/2007.

Questioni relative alla tutela della vita privata e alla protezione dei dati nell'installazione del sistema RFID

20. Per comprendere meglio le conseguenze dei sistemi RFID per la tutela della vita privata e la protezione dei dati, si possono distinguere cinque questioni di base in materia di riservatezza e sicurezza.

21. La prima questione è l'identificazione della persona interessata. Oltre sessanta anni fa, lo scopo dell'etichetta RFID era «identificare l'amico o il nemico» in arrivo. Attualmente i sistemi RFID possono non solo individuare gli elementi generali di un oggetto, ma possono anche in ultima analisi condurre all'identificazione di una persona e necessitano pertanto di farlo in un modo che tenga conto della protezione dei dati.

22. La seconda questione è l'identificazione del o dei responsabili del trattamento. Nel caso dei sistemi RFID, l'identificazione del responsabile del trattamento quale definito all'articolo 2, lettera d), della direttiva sulla protezione dei dati, potrebbe risultare più difficile e necessitare pertanto di un esame più approfondito. Identificare tuttavia il responsabile del trattamento resta una fase cruciale per stabilire le responsabilità di ciascuno dei soggetti interessati che dovranno rispettare il quadro normativo in materia di protezione dei dati. Durante il ciclo di vita dell'etichetta, il responsabile del trattamento che elabora i dati potrebbe cambiare diverse volte sulla base dei servizi aggiuntivi che potranno essere forniti in relazione all'oggetto munito di etichetta.

23. La terza questione riguarda la progressiva perdita di significato della tradizionale distinzione tra la sfera personale e quella pubblica. Sebbene anche in passato la distinzione tra gli spazi pubblico e privato non sia sempre stata precisa, la maggior parte delle persone è consapevole dei limiti esistenti tra gli stessi (nonché delle zone grigie) e prende decisioni informate o intuitive su come agire di conseguenza. Secondo Hall ([1]), lo spazio personale si traduce di solito nella distanza fisica dagli altri. La gestione della vita privata può anche essere considerata un processo dinamico di definizione di limiti ([2]). Non sorprende pertanto che la natura senza fili della comunicazione tag nonché la sua capacità di lettura al di fuori della linea di visibilità sollevi preoccupazioni in relazione alla vita privata offuscando questi limiti tradizionali e la loro gestione. Si teme infatti che le persone possano perdere parzialmente o interamente il controllo della gestione delle distanze di cui hanno finora usufruito. Di conseguenza, la gamma di lettura delle prime applicazioni dei sistemi RFID è stata ugualmente oggetto di attenzione da parte dei promotori e dei detrattori.

24. La quarta questione deve trattare le dimensioni e le proprietà fisiche delle etichette RFID. Poiché le etichette devono essere sostanzialmente di piccole dimensioni ed economiche, le misure di sicurezza che potrebbero essere messe in atto in questa parte del sistema RFID saranno per definizione limitate. Tuttavia l'aspetto senza fili della comunicazione aggiunge altresì un livello di rischio rispetto alla comunicazione cablata e pertanto sono necessari ulteriori requisiti di sicurezza.

25. La quinta questione è la mancanza di trasparenza del trattamento. I sistemi RFID possono condurre inavvertitamente alla raccolta e al trattamento di informazioni suscettibili di essere utilizzare per determinare il profilo di una persona. Questa conseguenza può essere molto bene illustrata paragonando i sistemi RFID al telefono cellulare, un confronto che è fatto più spesso. Da una parte, il telefono cellulare trae vantaggio da un livello molto elevato di accettazione delle tecnologie indipendentemente dai rischi potenzialmente intrusivi della vita privata. Si potrebbe concludere che la RFID sarà accettata allo stesso modo. Dall'altra, è doveroso sottolineare che un telefono cellulare è un oggetto visibile che è ancora sotto il controllo dell'utente finale in quanto può essere spento. Questo non si verifica per la RFID.

26. Sebbene la raccolta e il trattamento inavvertiti delle informazioni sopra citati possano essere legittimi, è anche possibile e in varie circostanze anche abbastanza probabile che si verifichino la raccolta e il trattamento illegittimi di tali dati.

27. Le precisazioni del presente capo giustificano la seguente conclusione. Il vasto utilizzo della tecnologia RFID è essenzialmente nuovo e può avere un impatto fondamentale sulla nostra società e sulla protezione dei diritti fondamentali nella nostra società, come la tutela della vita privata e la protezione dei dati. La RFID può comportare un cambiamento qualitativo.

IV. PRECISAZIONE DELLE CONSEGUENZE

Introduzione

28. Il presente capo si incentrerà principalmente sull'impatto della RFID sulla tutela dei diritti fondamentali nella nostra società, come la tutela della vita privata e la protezione dei dati personali. Questo sarà precisato in due fasi, la prima è una breve descrizione del modo in cui sono tutelati questi diritti fondamentali in base al quadro normativo vigente; nella seconda, il GEPD approfondirà le possibilità di utilizzare pienamente detto quadro normativo. Questa volontà è stata introdotta nel parere sulla comunicazione relativa alla direttiva sulla protezione dei dati come «la piena applicazione delle attuali disposizioni della direttiva».

29. Il punto di partenza è il seguente: i nuovi sviluppi tecnologici, come i sistemi RFID, hanno un palese impatto sui requisiti per un quadro normativo efficace in materia di protezione dei dati. La necessità di una protezione efficace dei dati personali individuali può altresì imporre dei limiti all'uso di queste nuove tecnologie. L'interazione è pertanto duplice: la tecnologia influenza la legislazione e quest'ultima influenza la tecnologia ([3]).

([1]) Hall, E.T.,1966, *The Hidden Dimension* (1ª ed.), Garden City, N.Y: Doubleday.

([2]) Altman, I., 1975, *The Environment and Social Behaviour,* Brooks/Cole Monterrey.

([3]) Cfr. le osservazioni del GEPD del marzo 2006 sulla comunicazione della Commissione sull'interoperabilità delle basi dati europee, pubblicate nel sito web del GEPD.

Tutela dei diritti fondamentali

30. La tutela dei diritti fondamentali alla vita privata e alla protezione dei dati nell'ambito dell'Unione europea è garantita in primo luogo da un quadro normativo, che è necessario in quanto si tratta di diritti riconosciuti dall'articolo 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali nonché dall'articolo 7 e dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea. Il relativo quadro normativo per la protezione dei dati e la RFID consiste essenzialmente nella direttiva 95/46/CE sulla protezione dei dati e nella direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche ([1]).

31. Il quadro normativo generale per la protezione dei dati quale stabilito nella direttiva 95/46/CE si applica alla RFID nella misura in cui i dati trattati mediante i sistemi RFID rientrano nella definizione di dati personali. Mentre in taluni casi le applicazioni RFID trattano in modo chiaro i dati personali e rientrano senza dubbio nel campo di applicazione della direttiva sulla protezione dei dati, esistono anche applicazioni in cui l'applicabilità della direttiva sulla protezione dei dati può non essere così ovvia. Il parere n. 4/2007 del Gruppo di lavoro «Articolo 29» per la protezione dei dati sul concetto di dati personali intende contribuire a una comprensione più chiara e comunemente riconosciuta del concetto di dati personali e, così facendo, ridurre questa incertezza ([2]).

32. Per quanto riguarda la direttiva relativa alla vita privata e alle comunicazioni elettroniche, la situazione è la seguente. Finora, non è chiaro se questa direttiva riguardi le applicazioni RFID. Per tale motivo, la proposta della Commissione, del 13 novembre 2007, inerente alla modifica della direttiva contiene una disposizione volta a precisare che la direttiva riguarda di fatto alcune applicazioni RFID. Tuttavia, altre applicazioni RFID potrebbero non essere contemplate a causa della limitazione di questa direttiva al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche.

33. La protezione dei dati personali può essere integrata da una serie di strumenti di autoregolamentazione (quadro non normativo). L'utilizzo di detti strumenti è promosso attivamente nelle due direttive, in particolare all'articolo 27 della direttiva sulla protezione dei dati, la quale prevede che gli Stati membri e la Commissione incoraggino la redazione di codici di condotta volti a contribuire alla corretta attuazione della direttiva. Inoltre, gli strumenti di autoregolamentazione potrebbero contribuire in modo efficace all'attuazione delle misure di sicurezza richieste all'articolo 17 della direttiva sulla protezione dei dati e all'articolo 14 della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

Piena attuazione del quadro in vigore

34. Il parere sulla comunicazione relativa alla direttiva sulla protezione dei dati elenca vari strumenti disponibili per una migliore attuazione della direttiva. La maggior parte degli strumenti non vincolanti di detto parere sono rilevanti per la RFID come comunicazioni interpretative o di altro tipo, promozione delle migliori pratiche, utilizzo di marchi di certificazione e audit sulla privacy da parte di terzi. La possibilità di adottare norme specifiche per la RFID sarà discussa nel capo V. È tuttavia possibile migliorare anche il quadro attuale.

Strumenti di autoregolamentazione

35. Il GEPD concorda con la Commissione che in una prima fase è opportuno lasciare spazio all'autoregolamentazione, consentendo alle parti interessate di creare rapidamente un ambiente giuridicamente conforme e contribuendo così a porre in essere un ambiente giuridico più sicuro.

36. Si prevede che la Commissione, in consultazione con il Gruppo delle parti interessate alla RFID, incentivi e indirizzi questo processo di autoregolamentazione. In tale contesto, il GEPD accoglie favorevolmente la raccomandazione annunciata nella comunicazione che dovrebbe contenere orientamenti specifici per fissare «i principi che le autorità pubbliche e le altre parti interessate saranno tenute a rispettare in relazione all'uso della RFID».

37. La comunicazione prevede che l'autoregolamentazione assuma la forma di un codice di condotta o di un codice di buone pratiche. Secondo il GEPD, indipendentemente da quale forma assumerà, l'autoregolamentazione dovrebbe:

— fornire orientamenti concreti e pratici su tipi specifici di applicazioni RFID e contribuire pertanto al rispetto del quadro normativo per la protezione dei dati,

— affrontare questioni e problemi specifici relativi alla protezione dei dati che sorgono nel contesto delle applicazioni RFID generiche,

— contribuire all'applicazione uniforme e armonizzata della direttiva sulla protezione dei dati in tutta l'UE, proprio in un settore che probabilmente utilizzerà lo stesso tipo di applicazioni RFID in tutta l'UE,

— essere applicata da tutte le parti interessate. Il mancato rispetto dovrebbe avere ripercussioni negative (eventualmente finanziarie).

([1]) Il punto 59 del presente parere discuterà della pertinenza di una terza direttiva, ossia la 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).

([2]) Cfr., tra l'altro, la pag. 10 del parere, citata nella nota in calce 5.

38. Il GEPD richiama l'attenzione su una questione in cui l'autoregolamentazione si rivelerà particolarmente utile. Per quelle applicazioni RFID che comportano il trattamento dei dati personali, la direttiva sulla protezione dei dati impone vari obblighi ai responsabili del trattamento, in particolare a norma dell'articolo 17 (sicurezza dei trattamenti) e dell'articolo 7 (necessità di trattare i dati solo in presenza delle opportune basi giuridiche). In virtù di queste disposizioni, i responsabili del trattamento devono da una parte istituire misure contro la divulgazione non autorizzata dei dati e, dall'altra, garantire che il trattamento, come la divulgazione di informazioni tramite i lettori, se del caso, avvenga solo con il consenso informato della persona cui si riferiscono i dati.

39. Queste disposizioni della direttiva sulla protezione dei dati possono essere interpretate nel senso di richiedere che le applicazioni RFID siano installate con le soluzioni tecniche necessarie per impedire o rendere minimi i rischi di divulgazione involontaria e garantire che il trattamento o il trasferimento di dati avvenga all'occorrenza unicamente con il consenso informato. Secondo il GEPD, l'esistenza di tale obbligo (ossia applicare le soluzioni tecniche necessarie per impedire o rendere minimi i rischi di divulgazione involontaria) e la natura vincolante per gli installatori delle applicazioni RFID, saranno ancora più forti e più chiari se questo requisito è ripreso nell'imminente codice di condotta o del codice di buone pratiche sopra citati. Per questi motivi, il GEPD consiglia vivamente che la raccomandazione della Commissione includa tale interpretazione della direttiva sulla protezione dei dati, sottolineando l'esistenza dell'obbligo di installare le applicazioni RFID con le necessarie misure tecnologiche per impedire la raccolta o la divulgazione involontarie di informazioni.

La necessità di un orientamento

40. Il GEPD raccomanda che la Commissione, in stretta cooperazione con il gruppo di esperti RFID, presenti uno o più documenti che forniscano orientamenti chiari su come applicare l'attuale quadro normativo al contesto della RFID. Gli orientamenti dovrebbero prevedere modalità pratiche per il rispetto dei principi illustrati nella direttiva sulla protezione dei dati e nella direttiva relativa alla vita privata e alle comunicazioni elettroniche. Per quanto concerne l'approccio globale degli orientamenti e i loro contenuti concreti, il GEPD avanza i seguenti suggerimenti.

41. Gli orientamenti che illustrano i principi applicabili in relazione all'utilizzo della RFID dovrebbero essere sufficientemente focalizzati nonché adottare un approccio settoriale specifico. Un approccio omnicomprensivo non rispetterà gli obiettivi ricercati per garantire un quadro chiaro e coerente. Al contrario, la portata degli orientamenti deve essere limitata ad applicazioni settoriali RFID ben definite.

42. Inoltre, gli orientamenti dovrebbero proporre metodi pratici ed efficaci per elaborare tecniche e norme che possano contribuire al rispetto da parte dei sistemi RFID del quadro normativo in materia di protezione dei dati e che comportino l'utilizzo della tecnologia «privacy by design».

43. Nell'applicare il quadro normativo vigente all'ambiente RFID, deve essere prestata un'attenzione particolare all'applicazione dei principi e degli obblighi in materia di protezione dei dati che si applicano ai responsabili del trattamento delle applicazioni RFID. Particolarmente rilevanti sono i seguenti obblighi e principi:

— il diritto al principio di informazione, compreso il diritto di sapere quando sono raccolti i dati tramite lettori e in casi appropriati quando i prodotti sono muniti di etichetta,

— la nozione di consenso come uno delle basi giuridiche per il trattamento dei dati. Questa nozione si concretizza nell'obbligo di disattivare le etichette RFID al punto di vendita, a meno che il soggetto interessato non abbia fornito il proprio consenso ([1]). Il diritto di disattivare le etichette RFID serve inoltre agli scopi di garantire la sicurezza delle informazioni, ossia garantire che i dati trattati mediante le etichette RFID non siano divulgati involontariamente a terzi,

— il diritto delle persone di non essere oggetto di decisioni contrarie basate unicamente sul trattamento automatizzato di un profilo personale definito.

44. Per quanto riguarda il diritto alle informazioni, gli orientamenti dovrebbero stabilire che alle persone devono essere fornite le informazioni che riguardano il trattamento dei loro dati personali. In particolare le stesse dovrebbero essere avvisate, fra l'altro, i) della presenza di lettori e della presenza di etichette RFID attivate sui prodotti o sui loro imballaggi; ii) delle conseguenze di tale presenza in termini di informazioni raccolte e iii) degli scopi per cui le informazioni raccolte sono destinate a essere utilizzate.

45. L'utilizzo di logo può essere idoneo quale misura per fornire informazioni. I logo possono essere utilizzati per avvisare delle presenza di lettori e di etichette RFID che si suppone rimangano attivi. Tuttavia, il solo utilizzo di logo non sarà sufficiente per garantire il corretto trattamento delle informazioni; occorre pertanto che le informazioni siano fornite alle persone interessate in modo chiaro e comprensibile. L'utilizzo di logo dovrebbe essere considerato una misura per integrare la fornitura di informazioni più dettagliate.

([1]) Cfr., più in dettaglio, i punti da 46 a 50 del presente parere.

Il principio di base: l'«opt in»

46. Per tutte le applicazioni RFID pertinenti le soluzioni dovrebbero rispettare ed attuare come requisito preliminare il principio «opt in» al punto di vendita. Consentire alle etichette RFID di continuare a trasmettere informazioni dopo il punto di vendita sarebbe illegale, a meno che il responsabile del trattamento non abbia motivazioni giuridiche appropriate. Di regola le sole motivazioni giuridiche appropriate sarebbero a) l'accordo della persona interessata o b) se la divulgazione è necessaria per prestare un servizio, o in seguito ad una richiesta specifica e spontanea della persona in questione ([1]). Entrambe le motivazioni giuridiche sarebbero pertanto considerate come «opt in».

47. Nel quadro del principio «opt in», le etichette dovrebbero essere disattivate al punto di vendita, a meno che la persona che ha acquistato il prodotto su cui è apposta l'etichetta decida di mantenerla attivata. Nel caso si avvalga del diritto di lasciare attivata l'etichetta, la persona acconsente all'ulteriore trattamento dei suoi dati, ad esempio alla trasmissione dei dati al lettore in occasione della sua prossima visita presso il responsabile del trattamento.

48. Al fine di far fronte alla diversità crescente delle applicazioni RFID e di facilitare lo sviluppo di nuovi modelli aziendali innovativi il GEPD sottolinea l'importanza di un approccio flessibile. Occorre prevedere un grado di flessibilità nell'attuazione di principio «opt in».

49. Le opzioni per l'applicazione del principio «opt in» sono molteplici. Ad esempio, in alternativa all'asportazione dell'etichetta si potrebbe prevedere un blocco, una disattivazione temporanea o, in base ad un modello di sicurezza chiamato «resurrecting duckling» ([2]), l'assegnazione ad un utente specifico. Nel caso di un'etichetta con un ciclo di vita breve, l'indirizzo che rimanda ad informazioni conservate in una banca dati potrebbe anche essere cancellato dalla banca dati di riferimento, evitando ulteriori trattamenti di dati supplementari raccolti dall'etichetta.

50. In conclusione, malgrado il GEPD ritenga che il principio «opt in» al punto di vendita sia un obbligo giuridico che già esiste nel quadro della direttiva sulla protezione dei dati nella maggior parte delle situazioni, è opportuno precisare tale obbligo negli strumenti di autoregolamentazione, anche al fine di garantire che il principio si attuato nel modo più appropriato. In ogni caso, un'attuazione specifica è necessaria per le applicazioni RFID che non rientrano nel campo di applicazione della direttiva sulla protezione dei dati.

L'esigenza della «privacy by design»

51. Al fine di ridurre al minimo le minacce per la protezione dei dati e la vita privata, la comunicazione della Commissione appoggia, a pag. 6, sezione 3.2, l'idea di precisare ed adottare tempestivamente dei criteri di progettazione. Il GEPD è favorevole a tale impostazione. In effetti, l'adozione di specifiche tecniche e di criteri di progettazione, altrimenti denominati «migliori tecnologie disponibili» (BAT) contribuirà efficacemente a soddisfare i requisiti in materia di normative sulla protezione dei dati e di sicurezza. L'individuazione di criteri tecnologici ed organizzativi, se aggiornata con frequenza, rafforzerà il modello che concilia i requisiti in materia di vita privata e di sicurezza che l'Unione europea sta elaborando.

52. Una corretta definizione di BAT in materia di tutela della vita privata e sicurezza per i sistemi RFID sarà inoltre decisiva ai fini della creazione di un clima di fiducia che rafforzerà il consenso tra gli utenti finali, nonché per la competitività dell'industria europea.

53. Il processo di selezione delle BAT per i sistemi RFID dovrebbe essere alimentato da valutazioni di impatto sulla vita privata e la sicurezza, per le quali occorre ancora compiere degli sforzi. Il GEPD ritiene che l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) insieme con i Centri comuni di ricerca della Commissione europea, associati ai pertinenti soggetti interessati dell'industria del settore, possono contribuire alla definizione di tali migliori prassi ed allo sviluppo di tali metodologie. Con il recente avvio del progetto «Orientamenti tecnici RFID», l'Ufficio federale tedesco per la sicurezza dell'informazione ha fornito un valido esempio illustrativo ([3]) di BAT che dovrebbero essere elaborate attualmente a livello europeo.

54. La normalizzazione può anch'essa svolgere un ruolo decisivo nell'adozione del principio della «privacy by design». La Commissione dovrebbe pertanto contribuire all'adozione di misure per la tutela della vita privata e dei dati nell'elaborazione di norme internazionali RFID. Nel suo documento di lavoro sulla RFID ([4]), il gruppo dell'articolo 29 ha chiaramente illustrato la possibilità che le norme contribuiscano all'elaborazione di sistemi RFID rispettosi della vita privata.

([1]) Per alcune applicazioni RFID è possibile addurre altri motivi, quali l'articolo 7, lettera f) (interessi legittimi del responsabile, soggetti a garanzie adeguate).

([2]) Il nome di questo modello elaborato da Frank Stajano e Ross Anderson dell'Università di Cambridge si ispira alla teoria secondo cui un anatroccolo riconosce come sua madre il primo oggetto in movimento che vede subito dopo la nascita.

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Documento di lavoro (WP 105) sulle questioni relative alla protezione dei dati nell'ambito delle tecnologie RFID, 19 gennaio 2005.

55. Il GEPD si rallegra inoltre della posizione adottata dalla Commissione riguardo alla ricerca e allo sviluppo di tecnologie RFID ed alla necessità di ridurre i rischi correlati alla vita privata. Occorre in effetti introdurre il principio della «privacy by design» nelle primissime fasi di sviluppo delle tecnologie, in modo da contribuire in modo più efficace all'osservanza del quadro giuridico della protezione dei dati. Come brevemente illustrato nella sua relazione annuale per il 2006, il GEPD parteciperà a tale sforzo fornendo, caso per caso, pareri e consulenze riguardo a progetti nell'ambito del settimo programma quadro (2007-2013).

V. SONO NECESSARIE MISURE LEGISLATIVE SPECIFICHE?

56. L'autoregolamentazione potrebbe non essere sufficiente ai fini della piena attuazione del quadro esistente per la protezione dei dati e per la tutela della vita privata. Anche se l'autoregolamentazione soddisfa i requisiti menzionati in precedenza, la sua applicazione è volontaria ed i casi di inosservanza non possono sempre essere sanzionati efficacemente. Inoltre, possono sempre essere necessarie misure legislative vincolanti al fine di garantire la protezione del diritto dei singoli alla tutela della vita privata ed alla protezione dei dati. Questo è ancor più necessario in caso di mancata applicazione dell'autoregolamentazione.

57. Una questione chiave è la determinazione degli strumenti giuridici necessari per assicurare che le applicazioni RFID siano diffuse efficacemente e corredate delle soluzioni tecniche necessarie per evitare o ridurre al minimo i rischi in materia di protezione dei dati e di tutela della vita privata, e che i responsabili del trattamento dei dati adottino misure adeguate per far fronte ai loro obblighi nell'ambito dei quadri giuridici esistenti. Ciò solleva quesiti supplementari:

— sono necessarie regole specifiche?

— in caso affermativo, è possibile adottare tali regole nell'ambito del quadro normativo vigente, ad esempio facendo ricorso alle procedure di comitato esistenti?

— oppure è necessario un nuovo strumento legislativo per assicurare una diffusione efficace dell'applicazione RFID che incorpori tecnologie per aumentare la tutela della vita privata?

58. Il presente capo esaminerà le possibilità di introdurre misure legislative vincolanti nell'ambito del quadro giuridico vigente, mentre il capo VI tratterà, in quanto si tratta di una questione separata, la necessità di un nuovo strumento legislativo.

59. In primo luogo, occorre riservare particolare attenzione alle disposizioni di cui all'articolo 17 della direttiva 95/46/CE, all'articolo 14, paragrafo 3, della direttiva 2002/58/CE ed all'articolo 3, paragrafo 3, lettera c), della direttiva 1999/5/CE. L'articolo 14, paragrafo 3, consente agli Stati membri di adottare 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 ([1]). La direttiva 1999/5/CE prevede all'articolo 3, paragrafo 3, lettera c), che la Commissione — ricorrendo alla procedura di comitato — 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 e dell'abbonato. Sinora non è stato fatto ricorso all'articolo 3, paragrafo 3, lettera c), della direttiva 1999/5/CE.

60. Tali disposizioni danno al legislatore — a livello nazionale e comunitario — competenze per imporre l'inclusione di misure per la tutela della vita privata e la protezione dei dati nell'elaborazione dei sistemi RFID, un concetto noto come «privacy by design» ([2]). Si invita inoltre ad utilizzare le «migliori tecnologie disponibili».

61. Al fine di rendere obbligatorio il concetto di «privacy by design», il GEPD raccomanda alla Commissione di utilizzare il meccanismo di cui all'articolo 3, paragrafo 3, lettera c), della direttiva 1999/5/CE, in consultazione con il gruppo di esperti sulla RFID.

62. In secondo luogo, è possibile precisare l'applicazione del quadro normativo vigente alle RFID mediante modifiche delle direttive stesse. Come osservato in precedenza, la Commissione ha appena presentato una proposta di modifica della direttiva relativa alla vita privata e alle comunicazioni elettroniche, che contiene una nuova disposizione in tal senso. Il GEPD si compiace di questa prima conferma dell'applicabilità della direttiva alla RFID. Il GEPD si occuperà di questioni specifiche emerse nell'ambito del rapporto tra, da un lato, la direttiva relativa alla vita privata e alle comunicazioni elettroniche e dall'altro, la RFID nel suo parere relativo alla proposta di modifica, che sarà pubblicato all'inizio del 2008.

63. Tenuto conto del fatto che la Commissione non prevede modifiche della direttiva sulla protezione dei dati in un prossimo futuro ([3]), le possibilità di inserire specifiche relative all'applicazione del quadro normativo vigente nella RFID sono limitate.

VI. È NECESSARIO UN QUADRO GIURIDICO SPECIFICO PER LA RFID?

Intenzioni della Commissione

64. La comunicazione ([4]) sottolinea l'importanza della sicurezza e della «privacy by design». Richiede altresì il coinvolgimento di tutte le parti interessate. Il principale risultato delle attività della Commissione sarà la pubblicazione di

([1]) E conformemente alla decisione 87/95/CEE del Consiglio, del 22 dicembre 1986, relative alla normalizzazione nel settore delle tecnologie dell'informazione e delle comunicazioni (GU L 36 del 7.2.1987, pag. 31).
([2]) Vedasi capitolo IV.
([3]) Il GEPD sostiene tale impostazione. Cfr. punto 64.
([4]) Cfr. punto 4.1 della comunicazione.

una raccomandazione nella quale fisserà «i principi che le autorità pubbliche e le altre parti interessate saranno tenute a rispettare in relazione all'uso della RFID». La raccomandazione sarà probabilmente adottata nella primavera del 2008. Le proposte legislative ambiziose menzionate nella comunicazione comportano due fasi. La Commissione intende:

— esaminare disposizioni appropriate in materia di RFID nell'imminente proposta di modifica della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Come osservato in precedenza, la Commissione ha proposto tale modifica della direttiva relativa alla vita privata e alle comunicazioni elettroniche nel novembre 2007, confermando l'applicabilità della direttiva alla RFID ([1]), ma senza proporre l'ampliamento del campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche alle reti private,

— valutare la necessità di ulteriori misure legislative per la protezione dei dati e la tutela della vita privata.

65. Sulla scorta di tale politica ci si attende che la Commissione non preveda — almeno non a breve — di proporre una nuova legislazione specifica ai fini della protezione dei dati e della tutela della vita privata nel settore della RFID.

Parametri per il legislatore

66. Nel suo parere sulla comunicazione relativa alla direttiva sulla protezione dei dati, il GEPD ha elencato una serie di attività legislative relative al trattamento dei dati personali che può essere così riassunta:

— in primo luogo, è opportuno mantenere i principi della protezione dei dati: «Non occorrono nuovi principi, ma sono chiaramente necessarie altre misure amministrative che, da un lato, siano efficaci e adeguate a una società collegata in rete e, dall'altro, riducano i costi amministrativi» ([2]),

— in secondo luogo, le proposte dovrebbero essere presentate solo in caso di necessità e proporzionalità sufficientemente comprovate. Per tale ragione, il quadro normativo generale per la protezione dei dati non dovrebbe subire modifiche a breve termine,

— in terzo luogo, gli sviluppi nella società possono condurre a quadri giuridici specifici al fine di adeguare i principi contenuti nella direttiva sulla protezione dei dati a questioni poste da tecnologie specifiche, quali la RFID. È chiaro che anche in questo contesto le condizioni di necessità e di proporzionalità devono essere soddisfatte.

67. Successivamente, è utile precisare le aspettative cui il legislatore deve far fronte nel settore della RFID:

— la legislazione deve essere flessibile e lasciare spazio all'innovazione ed allo sviluppo tecnologico. Ciò dovrebbe condurre ad una legislazione che sia sufficientemente neutra da un punto di vista tecnologico,

— In secondo luogo, la legislazione deve garantire la certezza del diritto. Ciò dovrebbe condurre ad una legislazione che sia sufficientemente specifica. Le parti interessate devono sapere esattamente in che modo il loro comportamento è disciplinato,

— In terzo luogo, la legislazione deve proteggere efficacemente tutti gli interessi legittimi degli interessati. Ciò richiede in ogni caso l'applicazione della legislazione ed una chiara definizione delle responsabilità: quale parte è responsabile di quale comportamento ([3])? Tali requisiti sono ancora più fondamentali allorché la tutela della vita privata e la protezione dei dati sono in gioco, diritti fondamentali della persona ai sensi della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e della Carta dei diritti fondamentali dell'Unione europea.

Punto di vista del GEPD

68. Secondo il GEPD è chiaro che non tutti gli sviluppi tecnologici richiedono una reazione del legislatore europeo. Gli sviluppi tecnologici possono procedere rapidamente, mentre l'adozione e l'entrata in vigore della legislazione richiede tempo, com'è giusto che avvenga. La legislazione dovrebbe essere il risultato di un equilibrio tra tutti gli interessi in gioco. Quando si sceglie lo strumento della direttiva, è necessario ancora più tempo, poiché le direttive devono essere recepite integralmente nei sistemi giuridici degli Stati membri.

69. Tuttavia, la RFID non è soltanto uno sviluppo tecnologico in più, come è stato sottolineato a più riprese in questo parere. La comunicazione fa riferimento alla RFID quale porta d'ingresso verso una nuova fase di sviluppo della società dell'informazione, spesso denominata «internet degli oggetti», e le etichette RFID costituiranno elementi fondamentali dei contesti di «intelligenza ambientale». Tali contesti sono anche fasi importanti nello sviluppo di quella che spesso viene definita come la «società della sorveglianza» ([4]). In tale contesto, un'azione legislativa nel settore della RFID può essere giustificata. La RFID può comportare un cambiamento qualitativo.

([1]) Cfr. a tale riguardo il nuovo articolo 3 proposto per la direttiva 2002/58/CE.

([2]) Punto 24 del parere sulla comunicazione relativa alla direttiva sulla protezione dei dati.

([3]) Nella terminologia della protezione dei dati, ciò implica l'individuazione del «responsabile del trattamento dei dati».

([4]) Questo messaggio è stato ribadito in una dichiarazione delle autorità europea incaricate della protezione dei dati adottata a Londra il 2 novembre 2006 e disponibile (in inglese/francese) sul sito del GEPD:
http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. In tale prospettiva, il GEPD raccomanda di considerare l'adozione di una (proposta di) legislazione comunitaria che disciplini le questioni principali dell'utilizzo della RFID nei settori pertinenti qualora non abbia luogo una corretta attuazione del quadro giuridico vigente. Dopo l'entrata in vigore, tale misura legislativa deve essere considerata come una lex specialis rispetto al quadro generale relativo alla protezione dei dati.

71. L'adozione di uno strumento legislativo siffatto comporterebbe i vantaggi seguenti:

— lo strumento potrebbe stabilire i parametri sostanziali per i meccanismi di autoregolamentazione,

— la prospettiva dell'adozione di uno strumento legislativo potrebbe rivelarsi un incentivo efficace per indurre che induca le parti interessate a porre in essere meccanismi di autoregolamentazione che offrano una protezione accurata.

72. Per questioni di praticità si potrebbe chiedere alla Commissione di preparare un documento di consultazione sui vantaggi e gli svantaggi di una legislazione specifica, nonché degli elementi principali di tale legislazione. Ovviamente si potrebbe chiedere alle parti interessate di fornire un contributo a tale consultazione. Analogamente, il gruppo dell'articolo 29 potrebbe essere anch'esso coinvolto.

Modalità possibili

73. L'intervento del legislatore potrebbe fornire un quadro giuridico su misura, che consiste in un insieme di strumenti giuridici che precisano ed integrano il quadro giuridico esistente. Tale quadro giuridico su misura dovrebbe fondarsi sui principi noti in materia di protezione dei dati e dovrebbe concentrarsi sulla ripartizione delle responsabilità e sull'efficacia dei meccanismi di controllo.

74. Tale legislazione su misura potrebbe rivelarsi necessaria poiché non tutte le applicazioni RFID comportano il trattamento di dati personali. In altri termini, se le applicazioni RFID non comportano il trattamento di dati personali, le parti coinvolte nella fabbricazione e nella vendita di prodotti che utilizzano la RFID non sono obbligate per legge ad applicare misure tecnologiche che impediscano l'intercettazione o la creazione di dispositivi di lettura senza informarne adeguatamente le persone. Tuttavia, come dimostrato, i rischi per la vita privata derivanti dall'eventuale sorveglianza delle persone si pongono anche per questo tipo di applicazioni RFID, per cui si rendono necessarie misure analoghe di tutela della vita privata. Proprio questo potrebbe avvenire nel caso dell'etichettatura dei singoli articoli di prodotti di consumo prima del punto di vendita. In sintesi, anche le applicazioni RFID che non prevedono il trattamento di dati personali possono costituire una minaccia alla vita privata delle persone consentendo una sorveglianza occulta e l'utilizzo di informazioni a fini inaccettabili.

75. Il GEPD ritiene necessario scongiurare tale spiacevole eventualità. Poiché l'attuale legislazione — almeno per quanto riguarda le applicazioni RFID che non prevedono il trattamento di dati personali — non è pienamente in grado di far fronte a tale minaccia, e tenuto conto delle carenze delle soluzioni di diritto non vincolanti, appare necessario ricorrere a misure legislative obbligatorie per garantire risultati soddisfacenti.

76. Tali misure dovrebbero in ogni caso:

— introdurre il principio «opt in» al punto di vendita come obbligo giuridico preciso ed irrevocabile, anche per le applicazioni RFID che non rientrano nel campo di applicazione della direttiva sulla protezione dei dati ([1]),

— garantire la diffusione obbligatoria delle applicazioni RFID con le caratteristiche tecniche appropriate o la «privacy by design».

VII. LA QUESTIONE DELLA GOVERNANCE

77. Sebbene nella comunicazione la dimensione «intrinsecamente transnazionale» dei sistemi RFID sia considerata unicamente nell'ambito del mercato interno, il GEPD ritiene che tale dimensione debba essere affrontata su un piano più internazionale. I sistemi RFID in vendita in un negozio sono già «transnazionali», poiché l'attività dell'etichetta potrebbe non interrompersi al punto di vendita. Sul piano del sistema RFID globale, tali tecnologie diventano inoltre «transfrontaliere» allorché il trasferimento di dati personali verso un paese terzo diventa possibile dal momento che il produttore dell'articolo etichettato, che fa parte del sistema RFID, ha sede al di fuori dell'Unione europea ([2]).

78. In una prospettiva più ampia, la governance delle basi di dati di riferimento delle identità RFID rappresenta anch'essa un aspetto cruciale ai fini di un'attuazione adeguata del quadro giuridico europeo in materia di protezione dei dati. Il GEPD invita a trovare una soluzione, poiché un ulteriore deterioramento di questo quadro non sarebbe accettabile.

79. Il GEPD prevede che la questione della governance della RFID sia una sfida fondamentale, che richiederà investimenti consistenti. Occorrerà trovare un consesso di negoziato appropriato e l'infrastruttura di gestione più opportuna al fine di garantire che i diritti di protezione dei dati siano adeguatamente rispettati in tali ambiti internazionali.

([1]) Nel capo IV si osservava che il principio «opt in» al punto di vendita è un obbligo giuridico già contemplato dalla direttiva sulla protezione dei dati.

([2]) Gli obblighi connessi al trasferimento di dati personali sono oggetto degli articoli 25 e 26 della direttiva sulla protezione dei dati.

80. In tale prospettiva il GEPD invita la Commissione ad esprimersi sulla questione della governance, possibilmente in consultazione con il gruppo delle parti interessate alla RFID.

VIII. **CONCLUSIONI**

81. Il GEPD si compiace della comunicazione della Commissione in materia di RFID in quanto affronta le principali questioni che sorgono nel contesto della diffusione della tecnologia RFID senza trascurare quelle determinanti relative alla tutela della vita privata e alla riservatezza dei dati. Concorda con il parere che i sistemi RFID potrebbero svolgere un ruolo chiave nello sviluppo della società dell'informazione generalmente denominata «Internet degli oggetti».

Chiarire le conseguenze

82. Il vasto utilizzo della tecnologia RFID è essenzialmente nuovo e può avere un impatto fondamentale sulla nostra società e sulla protezione dei diritti fondamentali nella nostra società, come la tutela della vita privata e la protezione dei dati. La RFID può comportare un cambiamento qualitativo.

83. È possibile individuare cinque questioni di fondo relative alla tutela della vita privata e della sicurezza:

— l'identificazione della persona interessata,

— l'identificazione del responsabile/dei responsabili del trattamento,

— la progressiva perdita di significato della tradizionale distinzione tra la sfera personale e quella pubblica,

— le conseguenze derivanti dalla dimensione e dalle proprietà fisiche delle etichette RFID,

— la mancanza di trasparenza nel trattamento.

Specificare le conseguenze

84. Il quadro normativo generale per la protezione dei dati quale stabilito nella direttiva 95/46/CE si applica alla RFID nella misura in cui i dati trattati mediante i sistemi RFID rientrano nella definizione di dati personali.

85. Per quanto riguarda la direttiva relativa alla vita privata e alle comunicazioni elettroniche: la proposta della Commissione, del 13 novembre 2007, relativa alla modifica della direttiva contiene una disposizione volta a precisare che la direttiva riguarda di fatto alcune applicazioni RFID. Tuttavia, talune applicazioni RFID potrebbero non essere contemplate a causa della limitazione di questa direttiva al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche.

86. La protezione dei dati personali può essere integrata da una serie di strumenti di autoregolamentazione. È opportuno lasciare spazio a tale autoregolamentazione, a condizione che:

— fornisca orientamenti concreti e pratici su tipi specifici di applicazioni RFID,

— affronti questioni e problemi specifici relativi e alla protezione dei dati che emergono nel contesto delle applicazioni RFID generiche,

— contribuisca all'applicazione uniforme ed armonizzata della direttiva sulla protezione dei dati in tutta l'UE,

— sia applicata da tutte le parti interessate.

87. Il GEPD raccomanda che la Commissione, in stretta cooperazione con il gruppo di esperti sulla RFID, elabori uno o più documenti che forniscano orientamenti chiari sulle modalità di applicazione dell'attuale quadro giuridico al contesto della RFID.

88. Occorre che gli orientamenti che stabiliscono i principi applicabili all'utilizzo della RFID siano sufficientemente specifici ed adottino un'impostazione per settore. Essi dovrebbero proporre metodi pratici ed efficaci per sviluppare tecniche e norme in grado di contribuire a far sì che i sistemi RFID siano conformi al quadro giuridico relativo alla protezione dei dati, e che prevedano il ricorso alla tecnologia «privacy by design».

89. Il GEPD si compiace dell'impostazione della comunicazione della Commissione, che appoggia l'idea di precisare ed adottare tempestivamente dei criteri di progettazione.

90. Sebbene il GEPD ritenga che il principio «opt in» al punto di vendita sia un obbligo giuridico già previsto nella direttiva sulla protezione dei dati nella maggior parte delle situazioni, tale obbligo dovrebbe essere precisato negli strumenti di autoregolamentazione.

Sono necessarie misure specifiche?

91. Al fine di rendere obbligatorio il concetto di «privacy by design», il GEPD raccomanda alla Commissione di utilizzare il meccanismo di cui all'articolo 3, paragrafo 3, lettera c), della direttiva 1999/5/CE, in consultazione con il gruppo di esperti sulla RFID.

92. Il GEPD raccomanda di considerare l'adozione di una (proposta di) legislazione comunitaria che disciplini le questioni principali dell'utilizzo della RFID nei settori pertinenti, qualora non venga attuato correttamente il quadro giuridico vigente. Dopo l'entrata in vigore, tale misura legislativa deve essere considerata come una lex specialis rispetto al quadro generale relativo alla protezione dei dati. Tale misura legislativa dovrebbe inoltre far fronte alle preoccupazioni in materia di tutela della vita privata e protezione dei dati che emergono da talune applicazioni RFID, come nel caso dell'etichettatura di singoli articoli prima del punto di vendita, che non necessariamente comportano il trattamento di dati personali.

93. La Commissione dovrebbe preparare un documento di consultazione sui vantaggi e gli svantaggi di normative specifiche, nonché sui loro elementi essenziali.

94. L'intervento del legislatore potrebbe fornire un quadro giuridico ad hoc, che consiste in un insieme di strumenti giuridici che precisano ed integrano il quadro giuridico esistente. Tali misure dovrebbero in ogni caso:

— introdurre il principio «opt in» al punto di vendita come obbligo giuridico preciso ed irrevocabile, anche per le applicazioni RFID che non rientrano nel campo di applicazione della direttiva sulla protezione dei dati ([1]),

— garantire la diffusione obbligatoria delle applicazioni RFID con le caratteristiche tecniche appropriate o la «privacy by design».

La questione della governance

95. Il GEPD invita la Commissione a esprimersi sulla questione della governance, possibilmente in consultazione con il gruppo delle parti interessate alla RFID.

Fatto a Bruxelles, il 20 dicembre 2007.

Peter HUSTINX

Garante europeo della protezione dei dati

([1]) Al capo IV si osserva che il principio «opt in» al punto di vendita è un obbligo giuridico già contemplato dalla direttiva sulla protezione dei dati.