

## RACCOMANDAZIONI

## COMMISSIONE

## RACCOMANDAZIONE DELLA COMMISSIONE

del 12 maggio 2009

**sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza***[notificata con il numero C(2009) 3200]*

(2009/387/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 211,

sentito il garante europeo della protezione dei dati,

considerando quanto segue:

- (1) L'identificazione a radiofrequenza (RFID) marca una nuova tappa nello sviluppo della società dell'informazione in cui oggetti muniti di dispositivi microelettronici in grado di analizzare dati in modo automatico saranno sempre più parte della vita quotidiana.
- (2) L'identificazione a radiofrequenza si sta progressivamente diffondendo e entrando a far parte della vita quotidiana dei singoli in una serie di ambiti quali la logistica <sup>(1)</sup>, la sanità, i trasporti pubblici, il commercio al dettaglio — in particolare allo scopo di migliorare la sicurezza e accelerare il richiamo dei prodotti — i divertimenti, il lavoro, la gestione dei pedaggi stradali, dei bagagli e dei documenti di viaggio.
- (3) La tecnologia RFID ha le potenzialità per divenire un nuovo catalizzatore della crescita e dell'occupazione e apportare quindi un notevole contributo alla strategia di Lisbona, trattandosi di un ambito estremamente promettente in termini economici che può consentire nuove opportunità imprenditoriali, riduzioni dei costi e aumento dell'efficienza, soprattutto per quanto riguarda la lotta alla contraffazione, la gestione dei rifiuti elettronici (e-waste), dei materiali pericolosi e dei prodotti alla fine del ciclo di vita.
- (4) La tecnologia RFID consente il trattamento dei dati, inclusi quelli personali, a breve distanza senza contatto

fisico o interazione visibile tra l'apparecchio di lettura e scrittura e l'etichetta, al punto che tale interazione può avvenire senza che il diretto interessato se ne renda conto.

- (5) Le applicazioni RFID consentono potenzialmente l'elaborazione di dati relativi a una persona fisica identificata o identificabile, direttamente o indirettamente. In particolare tali applicazioni permettono di elaborare i dati personali contenuti sull'etichetta, quali il nome, la data di nascita o l'indirizzo di una persona o i dati biometrici o ancora i dati che collegano il numero di un elemento RFID specifico a dati personali stoccati altrove nel sistema. Tale tecnologia, inoltre, potrebbe essere utilizzata per controllare singole persone che sono in possesso di uno o più elementi contenenti il numero di un elemento RFID.
- (6) Dato che la tecnologia RFID può essere utilizzata ovunque e è praticamente invisibile, nell'adottarla particolare attenzione va tributata agli aspetti di protezione dei dati e della vita privata. Di conseguenza, prima di un loro uso generalizzato, le applicazioni RFID dovrebbero incorporare caratteristiche di tutela della sicurezza della vita privata e delle informazioni (principio della «sicurezza e tutela della vita privata garantiti fin dalla fase di progettazione»).
- (7) La tecnologia RFID potrà assicurare la realizzazione dei numerosi vantaggi economici e sociali che promette solo se saranno messe in atto misure efficaci per garantire la protezione dei dati, la tutela della vita privata e principi etici collegati che sono fondamentali nel dibattito sull'accettazione della tecnologia RFID da parte dei cittadini.
- (8) Gli Stati membri e i cittadini, soprattutto nella fase iniziale di attuazione della RFID, dovrebbero adoperarsi per garantire che le applicazioni di tale tecnologia siano oggetto di controlli e che siano rispettati i diritti e le libertà individuali.

<sup>(1)</sup> COM(2007) 607 definitivo.

- (9) La comunicazione della Commissione, del 15 marzo 2007, «L'identificazione a radiofrequenza (RFID) in Europa: verso un quadro politico» <sup>(1)</sup>, aveva preannunciato che la Commissione, con una o più raccomandazioni, avrebbe fornito chiarimenti e orientamenti sugli aspetti di protezione dei dati e tutela della vita privata delle applicazioni RFID.
- (10) I diritti e gli obblighi in materia di protezione dei dati personali e della libera circolazione di tali dati, quali stabiliti dalla 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 <sup>(2)</sup> e dalla 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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche) <sup>(3)</sup>, sono pienamente applicabili all'uso delle applicazioni di RFID che elaborano dati personali.
- (11) È opportuno applicare allo sviluppo delle applicazioni RFID i principi stabiliti dalla 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 <sup>(4)</sup>.
- (12) Il parere del garante europeo della protezione dei dati <sup>(5)</sup> fornisce orientamenti sulle modalità di trattamento dei prodotti contenenti etichette forniti ai singoli e invita a effettuare una valutazione del loro impatto sulla sicurezza e sulla vita privata al fine di individuare e elaborare le «migliori tecnologie disponibili» per garantire che i sistemi RFID tutelino la vita privata e la protezione dei dati.
- (13) I gestori di applicazioni RFID dovrebbero adottare tutte le misure ragionevoli per garantire che i dati non siano associabili a una persona fisica identificata o identificabile mediante uno qualsiasi dei sistemi che potrebbero essere usati da un gestore di applicazioni RFID o da un'altra persona, a meno che tali dati siano elaborati in conformità dei principi e delle norme legali applicabili in materia di protezione dei dati.
- (14) La comunicazione della Commissione al Parlamento europeo e al Consiglio, del 2 maggio 2007, sulla «promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET)» <sup>(6)</sup> stabilisce interventi chiari per conseguire l'obiettivo di minimizzare il trattamento di dati privati mediante l'utilizzo, ogniqualvolta possibile, di dati anonimi o pseudonimi favorendo lo sviluppo delle tecnologie di rafforzamento della tutela della vita privata e il loro uso da parte dei responsabili del controllo dei dati e dei singoli.
- (15) La comunicazione della Commissione, del 31 maggio 2006, «Una strategia per una società dell'informazione sicura — Dialogo, partenariato e responsabilizzazione» <sup>(7)</sup> riconosce che diversità, apertura, interoperabilità, fruibilità e concorrenza sono strumenti chiave per la sicurezza della società dell'informazione, sottolinea il ruolo degli Stati membri e delle amministrazioni pubbliche per migliorare gli interventi di sensibilizzazione e promuovere le migliori pratiche nel campo della sicurezza e invita gli operatori del settore privato a adottare iniziative per elaborare sistemi di certificazione della sicurezza a prezzi contenuti per prodotti, processi e servizi che rispondano ad esigenze comunitarie specifiche, in particolare in relazione alla vita privata.
- (16) La risoluzione del Consiglio, del 22 marzo 2007, su una strategia per una società dell'informazione sicura in Europa <sup>(8)</sup>, invita gli Stati membri a tributare la dovuta attenzione alla necessità di prevenire e combattere minacce nuove o esistenti alla sicurezza di reti di comunicazione elettronica.
- (17) Un quadro elaborato a livello europeo per realizzare valutazioni dell'impatto sulla vita privata e la protezione dei dati garantirà che le disposizioni della presente raccomandazione siano rispettate coerentemente in tutti gli Stati membri. Lo sviluppo di un tale quadro dovrebbe basarsi sulle pratiche e le esperienze esistenti maturate negli Stati membri, nei paesi terzi e sul lavoro svolto dall'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) <sup>(9)</sup>.
- (18) Rifacendosi alle pratiche e le esperienze esistenti maturate negli Stati membri e in paesi terzi, la Commissione garantirà lo sviluppo a livello comunitario di orientamenti sulla gestione della sicurezza delle informazioni per le applicazioni RFID. Gli Stati membri dovrebbero contribuire a tale processo e incoraggiare la partecipazione dei privati e delle autorità pubbliche.
- (19) Una valutazione degli impatti sulla protezione della vita privata e dei dati personali effettuata dall'operatore prima di realizzare un'applicazione RFID fornirà le informazioni necessarie ai fini dell'adozione di adeguate misure di protezione, che andranno poi monitorate e riviste in tutto il periodo di vita di un'applicazione RFID.
- (20) Nel settore del commercio al dettaglio una valutazione degli impatti sulla protezione della vita privata e dei dati personali dei prodotti contenenti etichette venduti ai consumatori dovrebbe fornire le necessarie informazioni per determinare eventuali minacce alla vita privata o alla protezione dei dati personali.

<sup>(1)</sup> COM(2007) 96 definitivo.

<sup>(2)</sup> GU L 281 del 23.11.1995, pag. 31.

<sup>(3)</sup> GU L 201 del 31.7.2002, pag. 37.

<sup>(4)</sup> GU L 91 del 7.4.1999, pag. 10.

<sup>(5)</sup> GU C 101 del 23.4.2008, pag. 1.

<sup>(6)</sup> COM(2007) 228 definitivo.

<sup>(7)</sup> COM(2006) 251 definitivo.

<sup>(8)</sup> GU C 68 del 24.3.2007, pag. 1.

<sup>(9)</sup> Articolo 2, paragrafo 1, del regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio (GU L 77 del 13.3.2004, pag. 1).

- (21) L'uso di norme internazionali, come quelle elaborate dall'Organizzazione internazionale per la standardizzazione (ISO), di codici di condotta e di migliori pratiche, conformi al quadro normativo della UE, può contribuire alla gestione delle misure in materia di sicurezza dell'informazione e di vita privata nel corso di tutti i processi aziendali basati sulle applicazioni RFID.
- (22) Le applicazioni RFID che hanno implicazioni per la popolazione, quali i biglietti elettronici sui trasporti pubblici, richiedono adeguate misure protettive. Le applicazioni RFID che hanno incidenza sui singoli perché, ad esempio, consentono il trattamento dei dati di identificazione biometrici o dei dati relativi alla salute, richiedono una particolare attenzione date le loro implicazioni in materia di sicurezza dell'informazione e vita privata.
- (23) La società nel suo complesso deve essere consapevole degli obblighi e dei diritti esistenti applicabili all'utilizzo delle applicazioni RFID. Gli operatori che fanno uso della tecnologia RFID hanno quindi la responsabilità di fornire ai singoli informazioni sull'uso delle applicazioni basate su di essa.
- (24) Sensibilizzare maggiormente l'opinione pubblica e le piccole e medie imprese (PMI) sulle caratteristiche e le possibilità della RFID farà sì che tale tecnologia possa rispondere alle aspettative in campo economico, riducendo al contempo i rischi di un suo utilizzo a detrimento dell'interesse pubblico e favorendone l'accettazione.
- (25) La Commissione contribuirà all'attuazione della presente raccomandazione in modo sia diretto che indiretto, favorendo il dialogo e la collaborazione tra le parti interessate, in particolare tramite il programma quadro per la competitività e l'innovazione, istituito dalla decisione n. 1639/2006/CE del Parlamento europeo e del Consiglio <sup>(1)</sup>, e il settimo programma quadro di ricerca (FP7), istituito dalla decisione n. 1982/2006/CE del Parlamento europeo e del Consiglio <sup>(2)</sup>.
- (26) Per favorire l'adozione delle tecnologie RFID a condizioni accettabili è necessario promuovere a livello comunitario la ricerca e lo sviluppo di tecnologie a basso costo per migliorare la tutela della vita privata e la sicurezza dell'informazione.
- (27) La presente raccomandazione rispetta i diritti fondamentali e osserva i principi sanciti in particolare dalla carta dei diritti fondamentali dell'Unione europea. In special modo la presente raccomandazione mira a garantire il pieno rispetto della vita privata e familiare e la protezione dei dati personali,

RACCOMANDA:

### Campo d'applicazione

1. La presente raccomandazione fornisce agli Stati membri orientamenti sulla progettazione e l'uso delle applicazioni RFID in modo giuridicamente, eticamente, socialmente e politicamente accettabile nel rispetto del diritto alla vita privata e garantendo la protezione dei dati personali.
2. La presente raccomandazione fornisce orientamenti sulle misure da adottare per l'introduzione di applicazioni RFID allo scopo di garantire, laddove applicabili, il rispetto delle legislazioni nazionali che attuano le direttive 95/46/CE, 1999/5/CE e 2002/58/CE in caso di introduzione di tali applicazioni.

### Definizioni

3. Ai fini della presente raccomandazione si applicano le definizioni di cui alla direttiva 95/46/CE. Si applicano inoltre le seguenti definizioni:
  - a) «identificazione a radiofrequenza» (RFID): l'uso di onde elettromagnetiche o l'accoppiamento di un campo reattivo nella porzione di radiofrequenza dello spettro per comunicare a partire da o verso un'etichetta mediante una varietà di sistemi di modulazione e codifica allo scopo di leggere, in modo univoco, l'identità di un'etichetta di radiofrequenza o altri dati in essa registrati;
  - b) «etichetta RFID» o «etichetta»: un dispositivo RFID in grado di produrre un segnale radio o un dispositivo RFID che riaccoppia, retrodiffonde o riflette (a seconda del tipo di dispositivo) e modula un segnale portante ricevuto da un apparecchio di lettura o di scrittura;
  - c) «apparecchio di lettura o apparecchio di scrittura RFID»: un dispositivo fisso o mobile per la cattura e l'identificazione di dati utilizzando un'onda elettromagnetica a radiofrequenza o l'accoppiamento di un campo reattivo per stimolare e eseguire una risposta modulata di dati da un'etichetta o gruppo di etichette;
  - d) «applicazione RFID» o «applicazione»: un'applicazione che effettua l'elaborazione di dati mediante l'uso di etichette e lettori e che si basa su un sistema back end all'interno di un'infrastruttura di comunicazione in rete;
  - e) «gestore di applicazioni RFID» o «gestore»: la persona fisica o giuridica, autorità pubblica o agenzia o qualsiasi altro organismo che, da solo, o congiuntamente con altri definisce le finalità e le modalità dell'utilizzo di un'applicazione, compresi i responsabili del trattamento dei dati personali che utilizzano un'applicazione RFID;

<sup>(1)</sup> GU L 310 del 9.11.2006, pag. 15.

<sup>(2)</sup> GU L 412 del 30.12.2006, pag. 1.

- f) «sicurezza delle informazioni»: mantenimento della riservatezza, dell'integrità e della disponibilità delle informazioni;
- g) «controllo»: qualsiasi attività effettuata allo scopo di individuare, osservare, copiare o registrare l'ubicazione, il movimento, le attività o lo stato di un singolo.

#### **Valutazione dell'impatto sulla protezione della vita privata e dei dati**

4. Gli Stati membri dovrebbero assicurarsi che l'industria, in cooperazione con le parti interessate della società civile, metta a punto un quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati e lo sottoponga al gruppo di lavoro «articolo 29» sulla protezione dei dati entro 12 mesi dalla pubblicazione della presente raccomandazione nella *Gazzetta ufficiale dell'Unione europea*.
5. Gli Stati membri dovrebbero garantire che gli operatori, fatti salvi i loro obblighi in virtù della direttiva 95/46/CE:
  - a) eseguano una valutazione delle implicazioni che l'introduzione delle applicazioni in oggetto ha per la protezione dei dati personali e della vita privata, verificando se tali applicazioni possano essere utilizzate per controllare singole persone. Il livello di accuratezza della valutazione dovrebbe essere adeguato ai rischi per la vita privata eventualmente associati all'applicazione;
  - b) adottare le misure tecniche e organizzative adeguate per garantire la protezione dei dati personali e della vita privata;
  - c) designare una persona o un gruppo di persone cui affidare la revisione delle valutazioni e la verifica della costante adeguatezza delle misure tecniche e organizzative adottate per garantire la protezione dei dati personali e della vita privata;
  - d) mettere la valutazione a disposizione delle autorità competenti almeno sei settimane prima di introdurre l'applicazione;
  - e) una volta disponibile il quadro per le valutazioni d'impatto sulla protezione dei dati e la tutela della vita privata, di cui al punto 4, attuare le disposizioni di cui sopra conformemente allo stesso.

#### **Sicurezza delle informazioni**

6. Gli Stati membri dovrebbero cooperare con la Commissione per identificare le applicazioni che potrebbero costi-

tuire una minaccia per la sicurezza delle informazioni con implicazioni per la popolazione. In relazione a tali applicazioni gli Stati membri dovrebbero assicurarsi che i gestori, di concerto con le autorità nazionali competenti e le organizzazioni della società civile, mettano a punto nuovi regimi, o applichino quelli esistenti, quali la certificazione o l'autovalutazione del gestore, per dimostrare che è stato adottato un adeguato livello di sicurezza delle informazioni e di protezione della vita privata a fronte di rischi individuati.

#### **Informazioni e trasparenza sull'uso della RFID**

7. Fatti salvi gli obblighi dei responsabili del trattamento dei dati, in conformità delle direttive 95/46/CE e 2002/58/CE, gli Stati membri dovrebbero garantire che i gestori elaborino e diffondano una politica informativa concisa, accurata e di facile comprensione per ciascuna delle loro applicazioni, che dovrebbe comprendere quantomeno:
  - a) l'identità e l'indirizzo dei gestori;
  - b) le finalità dell'applicazione;
  - c) i dati elaborati dall'applicazione, specificando in particolare se saranno elaborati dati personali e se sarà controllata l'ubicazione delle etichette;
  - d) una sintesi della valutazione d'impatto sulla tutela della vita privata e la protezione dei dati;
  - e) gli eventuali rischi per la vita privata relativi all'uso delle etichette nell'applicazione e le misure che i singoli possono adottare per ridurre tali rischi.
8. Gli Stati membri dovrebbero accertarsi che i gestori adottino misure per informare i singoli della presenza di lettori utilizzando un simbolo europeo comune messo a punto dagli organismi europei di normalizzazione con il sostegno delle parti interessate. Il simbolo dovrebbe indicare l'identità del gestore e un punto di contatto cui i singoli si possono rivolgere per procurarsi la politica informativa relativa all'applicazione.

#### **Applicazioni RFID utilizzate nel commercio al dettaglio**

9. Sulla base di un simbolo europeo comune messo a punto dagli organismi europei di normalizzazione con il sostegno delle parti interessate, gli operatori dovrebbero informare la popolazione della presenza di etichette sui prodotti o incorporate negli stessi.

10. Nell'effettuare la valutazione d'impatto sulla tutela della vita privata e la protezione dei dati, di cui ai punti 4 e 5, il gestore di un'applicazione dovrebbe determinare specificamente se le etichette collocate o incorporate nei prodotti venduti ai consumatori tramite commercianti al dettaglio che non sono gestori di tale applicazione rappresentino un'eventuale minaccia alla vita privata o alla protezione dei dati personali.
11. I commercianti al dettaglio dovrebbero disattivare o rimuovere nel punto di vendita le etichette usate nelle loro applicazioni, a meno che i consumatori, una volta informati della politica di cui al punto 7, acconsentano a mantenere le etichette operative. La disattivazione delle etichette va intesa come un qualsiasi processo che interrompe le interazioni di un'etichetta con l'ambiente circostante senza richiedere la partecipazione attiva del consumatore. La disattivazione o la rimozione delle etichette da parte del commerciante deve avvenire immediatamente e senza oneri per il consumatore. I consumatori dovrebbero essere in grado di verificare che la disattivazione o la rimozione dell'etichetta sono effettivamente avvenute.
12. Il punto 11 non dovrebbe applicarsi qualora la valutazione dell'impatto sulla protezione della vita privata e dei dati dimostri che le etichette utilizzate nelle applicazioni del commercio al dettaglio e che resteranno operative al di fuori del punto di vendita non rappresentano una probabile minaccia alla vita privata o alla protezione dei dati personali. I commercianti al dettaglio, tuttavia, dovrebbero mettere a disposizione gratuitamente strumenti di facile uso per disattivare o rimuovere immediatamente, o in una fase successiva, le etichette di cui trattasi.
13. La disattivazione o la rimozione delle etichette non dovrebbe comportare alcuna riduzione o cessazione degli obblighi legali del commerciante o del costruttore nei confronti dei consumatori.
14. I punti 11 e 12 dovrebbero applicarsi soltanto ai commercianti che sono anche gestori.

#### **Attività di sensibilizzazione**

15. Gli Stati membri, in cooperazione con l'industria, la Commissione e altre parti interessate, dovrebbero adottare misure appropriate per informare e sensibilizzare le autorità pubbliche e le imprese, soprattutto le PMI, sui benefici potenziali e sui possibili rischi associati all'uso delle tecnologie RFID. Particolare attenzione dovrebbe essere tributata agli aspetti della sicurezza delle informazioni e della vita privata.

16. Gli Stati membri, in cooperazione con l'industria, in cooperazione con le associazioni della società civile, la Commissione e altre parti interessate, dovrebbero identificare e fornire esempi di buone pratiche nell'attuazione delle applicazioni RFID per informare e sensibilizzare la popolazione. Essi dovrebbero inoltre adottare misure adeguate, quali progetti pilota su larga scala, per sensibilizzare maggiormente la popolazione sulle tecnologie RFID, i loro rischi, i benefici e le implicazioni del loro uso, prerequisito per una maggiore diffusione di tale tecnologia.

#### **Ricerca e sviluppo**

17. Gli Stati membri dovrebbero cooperare con l'industria, le parti interessate della società civile e la Commissione per stimolare e sostenere l'introduzione del principio della «sicurezza e tutela della vita privata garantiti fin dalla fase di progettazione» fin dalle prime fasi di elaborazione delle applicazioni RFID.

#### **Seguito**

18. Gli Stati membri dovrebbero adottare le misure necessarie per far conoscere la presente raccomandazione a tutte le parti interessate che partecipano alla progettazione e al funzionamento delle applicazioni RFID nella Comunità.
19. Gli Stati membri dovrebbero informare la Commissione, al più tardi 24 mesi dopo la pubblicazione della presente raccomandazione nella *Gazzetta ufficiale dell'Unione europea*, delle azioni avviate in reazione alla stessa.
20. Entro tre anni dalla pubblicazione della presente raccomandazione nella *Gazzetta ufficiale dell'Unione europea*, la Commissione presenterà una relazione sull'attuazione della stessa, sulla sua efficacia e l'impatto sugli operatori e i consumatori, in particolare per quanto riguarda le misure raccomandate ai punti da 9 a 14.

#### **Destinatari**

21. Gli Stati membri sono destinatari della presente raccomandazione.

Fatto a Bruxelles, il 12 maggio 2009.

*Per la Commissione*

Viviane REDING

*Membro della Commissione*