



**00066/10/IT**  
**WP 175**

**Parere 5/2010 sulla proposta dell'industria relativa a un quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID**

**adottato il 13 luglio 2010**

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e cittadinanza dell'Unione) della Commissione europea, direzione generale Giustizia, B -1049 Bruxelles, Belgio, ufficio LX-46 01/190.

Sito Internet: [http://ec.europa.eu/justice/policies/privacy/index\\_en.htm](http://ec.europa.eu/justice/policies/privacy/index_en.htm)

[NdT] Ai fini del presente parere, con "responsabile del trattamento" e con "incaricato del trattamento" si intendono rispettivamente il "titolare" e il "responsabile" di cui all'articolo 4, lettera f) e lettera g) del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali).

## Indice

1	Contesto.....	3
1.1	Introduzione.....	3
1.2	RFID e protezione dei dati .....	3
1.3	Obiettivi del quadro per la valutazione dell’impatto sulla privacy .....	5
1.4	Sintesi del quadro proposto .....	6
2	Analisi .....	7
2.1	Valutazione dei rischi.....	7
2.2	Etichette portate da persone.....	8
2.3	RFID nel settore del commercio al dettaglio.....	9
2.4	Altre osservazioni.....	10
3	Conclusione .....	11

# 1 Contesto

## 1.1 Introduzione

Il 12 maggio la Commissione europea ha formulato una raccomandazione sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza<sup>1</sup>.

Nel punto 4 della raccomandazione si dichiara che “[g]li 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” (sottolineatura aggiunta).

Conformemente alla raccomandazione, una volta definito tale quadro, gli Stati membri dovrebbero garantire che i gestori RFID eseguano una valutazione dell’impatto sulla protezione dei dati e della vita privata (“valutazione dell’impatto sulla privacy”) delle applicazioni RFID, prima di introdurle. Gli Stati membri dovrebbero inoltre garantire che i gestori RFID mettano a disposizione delle autorità competenti (ossia le autorità di protezione dei dati) le relazioni sulle valutazioni.

Nel luglio 2009 il "gruppo di lavoro informale RFID", guidato da rappresentanti dell'industria, ha iniziato a lavorare alla definizione di un quadro per la valutazione dell’impatto sulla privacy, organizzando nel contempo riunioni periodiche con le parti interessate (associazioni di consumatori, organismi di normazione e mondo accademico). Il 31 marzo 2010 i rappresentanti dell'industria hanno presentato al Gruppo di lavoro articolo 29, per approvazione, una proposta di quadro per la realizzazione di valutazioni d'impatto sulla protezione della vita privata e dei dati. **Il presente parere è la risposta formale del Gruppo alla proposta.**

Nel prosieguo, la raccomandazione della Commissione europea sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza, pubblicata il 12 maggio 2009, è denominata "raccomandazione RFID", e il quadro per la realizzazione di valutazioni d'impatto sulla protezione della vita privata e dei dati, presentato il 31 marzo 2010 al Gruppo di lavoro articolo 29 e riportato in allegato al presente parere, è denominato "quadro proposto" o semplicemente "quadro".

## 1.2 RFID e protezione dei dati

Nel gennaio 2005 il Gruppo di lavoro ha adottato un *documento di lavoro*<sup>2</sup> *sulle questioni relative alla protezione dei dati collegate alla tecnologia RFID* (WP 105), in cui, da un lato, riconosce gli indubbi vantaggi offerti dalla tecnologia RFID, e, dall'altro, evidenzia le potenziali preoccupazioni sotto il profilo della protezione dei dati suscitate in particolare dalla possibilità per le imprese e i governi di usare la

<sup>1</sup> [http://ec.europa.eu/information\\_society/policy/rfid/documents/recommendationonrfid2009.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf)

<sup>2</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp105\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf) (in inglese)

tecnologia RFID per intromettersi nella vita privata delle persone. Nel documento si osserva che la possibilità di raccogliere in modo surrettizio una varietà di dati riguardanti tutti una stessa persona, di seguirne gli spostamenti nei luoghi pubblici (aeroporti, stazioni ferroviarie, negozi), di arricchire i profili delle persone controllandone i comportamenti di consumo nei negozi, di leggere i dati particolareggiati dei vestiti e degli accessori che i clienti indossano o e dei medicinali che portano con sé sono tutti esempi di uso della tecnologia RFID che suscita preoccupazioni sotto il profilo della vita privata.

Il documento di lavoro è stato oggetto di una consultazione pubblica, i cui risultati sono riassunti in un documento del Gruppo di lavoro (WP 111)<sup>3</sup> pubblicato nel settembre 2005. Dalla consultazione è emerso che mentre le università, i gruppi di riflessione, i cittadini e le società di sicurezza auspicano perlopiù che il Gruppo di lavoro articolo 29 fornisca ulteriori orientamenti e alcuni suggeriscono addirittura di integrare la direttiva sulla protezione dei dati con norme specifiche sulla tecnologia RFID, l'industria propende per l'autoregolamentazione.

In questo contesto generale, e in coordinamento con le parti interessate (rappresentanti dell'industria RFID e associazioni per la protezione dei dati e dei diritti dei consumatori), la Commissione europea ha preso l'iniziativa formulando la citata raccomandazione *“sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza”*<sup>4</sup> diretta a fornire *“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”*.

La raccomandazione, pubblicata nel maggio 2009, contiene un'importante novità: fa obbligo ai gestori RFID di eseguire *“valutazioni dell'impatto sulla protezione della vita privata e dei dati”* prima di introdurre l'applicazione RFID e di mettere la valutazione a disposizione delle autorità competenti. Questo nuovo approccio, che integra il quadro normativo esistente disposto dalla direttiva sulla protezione dei dati e dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche, offre all'industria l'opportunità di dimostrare il potenziale dell'autoregolamentazione quale strumento flessibile, efficace e complementare rispetto al quadro normativo dell'UE in un panorama tecnologico in rapida evoluzione. Il Gruppo di lavoro appoggia<sup>5</sup> l'esecuzione di valutazioni d'impatto sulla vita privata, in particolare per determinate operazioni di trattamento dei dati che potrebbero presentare rischi specifici per i diritti e le libertà dell'interessato. Ritiene inoltre che il successo o l'insuccesso di tale approccio potrà aprire la strada a un uso delle valutazioni dell'impatto sulla privacy anche in altri settori oppure stimolare il ricorso a un approccio normativo.

La raccomandazione RFID intende inoltre promuovere *“informazioni e trasparenza sull'uso della RFID”*, in particolare tramite *“un simbolo europeo comune messo a punto dagli organismi europei di normalizzazione con il sostegno delle parti interessate”*, destinato a *“informare la popolazione della presenza di etichette”*. Tale iniziativa ha il pieno sostegno del Gruppo di lavoro.

---

<sup>3</sup> *“Risultati della consultazione pubblica relativa al documento 105 del Gruppo di lavoro articolo 29 sugli aspetti di protezione dei dati commessi alla tecnologia RFID”*,

[http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp111\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp111_en.pdf) (in inglese)

<sup>4</sup> [http://ec.europa.eu/information\\_society/policy/rfid/documents/recommendationonrfid2009.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf)

<sup>5</sup> Cfr. WP 168 *“Il futuro della vita privata: contributo congiunto alla consultazione della Commissione europea sul quadro normativo per il diritto fondamentale alla protezione dei dati personali”*

[http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2009/wp168\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf) (in inglese)

Sebbene la raccomandazione RFID faccia esplicito riferimento alla direttiva 95/46/CE, talvolta si discosta dalla terminologia tradizionalmente in uso in materia di protezione dei dati, specie quando utilizza i termini “persona”, “singolo” o “utente”. Per evitare ambiguità, nel presente parere con il termine “persona” si indicherà la “persona fisica” di cui all'articolo 2 della direttiva 95/46/CE mentre i termini “utente” e “singolo” mantengono il significato che hanno nella raccomandazione RFID. In particolare, il termine “persona” può indicare genericamente gli “utenti” e i “singoli”, che altrimenti costituiscono categorie di persone distinte conformemente alle definizioni di cui al punto 3 della raccomandazione (riprese dal quadro proposto). Per coerenza con la raccomandazione RFID, il presente parere usa il termine “gestori RFID” e non “responsabili del trattamento”, sebbene i due termini non siano strettamente equivalenti.

Nel novembre 2009 i legislatori europei hanno modificato la direttiva relativa alla vita privata e alle comunicazioni elettroniche<sup>6</sup> introducendo un riferimento esplicito alla tecnologia RFID. Nel considerando 56 della direttiva 2009/136/CE si riconosce che *"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"*, sottolineando tuttavia che *"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"*. Si precisa inoltre che *"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"*. Di conseguenza, il campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche (definito all'articolo 3) è stato rivisto per farvi rientrare *"le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati"*.

### **1.3 Obiettivi del quadro per la valutazione dell'impatto sulla privacy**

Con la raccomandazione RFID la Commissione europea ha istituito un processo di valutazione dell'impatto sulla privacy diretto a conseguire svariati vantaggi:

- In primo luogo, la valutazione dell'impatto sulla privacy dovrebbe favorire la cosiddetta *privacy by design* (ossia la tutela della vita privata fin dalla progettazione) aiutando i responsabili del trattamento ad affrontare gli aspetti di protezione della vita privata e dei dati prima che sia lanciato il prodotto o il servizio. Ciò genera vantaggi non solo per le persone ma anche per i responsabili del trattamento, in quanto si eviteranno gli ingenti costi (e le soluzioni spesso insoddisfacenti) che di frequente sorgono quando occorre conformare un prodotto già introdotto ai requisiti di privacy.

---

<sup>6</sup> Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.

- In secondo luogo, la valutazione dell'impatto sulla privacy dovrebbe aiutare i responsabili del trattamento ad affrontare in modo globale i rischi per la protezione della vita privata e dei dati. La valutazione dell'impatto sulla privacy è infatti uno degli strumenti che possono aiutare a valutare i rischi per la vita privata, a trovare soluzioni tecniche e organizzative per proteggere i dati personali dalla diffusione o dall'accesso non autorizzati e a rispettare gli altri obblighi di sicurezza imposti dall'articolo 17 della direttiva sulla protezione dei dati e dall'articolo 4 della direttiva 2002/58/CE modificata. Questo processo consente inoltre di ridurre l'incertezza giuridica e di evitare che i cittadini perdano fiducia, fattori che altrimenti potrebbero risultare gravosi per il responsabile del trattamento qualora gli aspetti di protezione dei dati non siano trattati in modo appropriato.
- Da ultimo, la valutazione dell'impatto sulla privacy potrebbe aiutare sia i responsabili del trattamento sia le autorità di protezione dei dati ad avere una conoscenza più approfondita degli aspetti delle applicazioni RFID correlati alla protezione della vita privata e dei dati. Facendo una valutazione dell'impatto sulla privacy i responsabili del trattamento dovrebbero riuscire a capire e attuare i principi sanciti dalla direttiva 95/46/CE, dalla direttiva 2002/58/CE modificata e dalla raccomandazione RFID. Le informazioni fornite dalla valutazione possono aiutare le autorità di protezione dei dati ad individuare le migliori prassi seguite dall'industria per attuare i principi di protezione dei dati, e, negli Stati membri che richiedono una verifica preventiva (di tutte o alcune) delle applicazioni RFID, possono semplificare il processo sia per le autorità di protezione dei dati sia per i responsabili del trattamento<sup>7</sup>.

Inoltre, il Gruppo di lavoro ritiene che lo sviluppo di valutazioni dell'impatto sulla privacy contribuisca alla competitività dell'industria RFID europea, potenziando approcci innovativi per far fronte agli aspetti di protezione dei dati e della vita privata tramite tecnologie quali l'anonimizzazione dei dati, la disattivazione parziale delle etichette, la crittografia leggera, ecc.

Sebbene il quadro per la valutazione dell'impatto sulla privacy previsto dalla raccomandazione sia diretto a promuovere il principio della "sicurezza e tutela della vita privata garantiti fin dalla fase di progettazione", in quanto riguarda le applicazioni RFID prima della loro introduzione, sono già molte le applicazioni RFID introdotte sul mercato. Il Gruppo di lavoro auspica che le parti interessate facciano tesoro di questa esperienza e colgano l'occasione per creare strumenti di valutazione che possano essere applicati anche alle applicazioni RFID esistenti.

## **1.4 Sintesi del quadro proposto**

Il quadro proposto innanzitutto classifica le applicazioni RFID in 4 livelli possibili. Le applicazioni di livello 0 sono sostanzialmente applicazioni RFID che non trattano dati personali e in cui le etichette sono soltanto manipolate dagli utenti; per tali applicazioni non è richiesta una valutazione dell'impatto sulla privacy. Sebbene il termine "utente" possa potenzialmente riferirsi ai dipendenti, la definizione di

---

<sup>7</sup> In questo contesto, il punto 5, lettera d), della raccomandazione RFID prevede che gli operatori, fatti salvi i loro obblighi in virtù della direttiva 95/46/CE, mettano la valutazione a disposizione delle autorità competenti almeno sei settimane prima di introdurre l'applicazione. Il modo in cui la valutazione debba essere messa a disposizione (ad esempio su richiesta) sarà stabilito dalle autorità nazionali di protezione dei dati. In particolare, possono essere presi in considerazione i rischi connessi all'applicazione e altri fattori quali la presenza di un incaricato della protezione dei dati.

“applicazione di livello 0” non può essere interpretata nel senso di ricomprendere le applicazioni previste per controllare i dipendenti, in quanto un controllo di questo tipo presuppone che l'applicazione conservi da qualche parte i dati personali. Di conseguenza, il Gruppo di lavoro concorda sul fatto che l'esclusione delle “applicazioni di livello 0” dal processo di valutazione dell'impatto sulla privacy non rischia di compromettere gli obiettivi di protezione dei dati e della vita privata.

Le applicazioni di livello 1 sono applicazioni che non trattano dati personali ma in cui i singoli portano con sé le etichette. Le applicazioni di livello 2 sono applicazioni che trattano dati personali ma in cui le etichette non contengono dati personali. Infine, le applicazioni di livello 3 sono applicazioni in cui le etichette contengono dati personali. Come si evidenzia al punto 2.4, nel quadro proposto l'uso del termine “dati personali” è piuttosto ambiguo quando si riferisce alle informazioni contenute nelle etichette.

Per le applicazioni RFID di livello 1, 2 o 3, il gestore RFID è tenuto a eseguire un'analisi suddivisa in quattro parti, con un livello di accuratezza proporzionato alle implicazioni individuate per la vita privata e i dati personali. Nella prima parte deve descrivere l'applicazione RFID, nella seconda evidenziare le misure di controllo e sicurezza, nella terza affrontare le questioni relative alle informazioni per gli utenti e ai loro diritti, e nella parte finale valutare se l'applicazione RFID è pronta o meno per essere introdotta. Alla fine del processo di valutazione dell'impatto sulla privacy, il gestore RFID dovrà presentare una relazione e metterla a disposizione dell'autorità competente.

Per le specifiche esigenze di alcuni settori, gli autori del quadro prevedono che l'industria possa tradurre il quadro in specifici “modelli di valutazione dell'impatto sulla privacy” per facilitarne l'esecuzione. La relazione sarà quindi elaborata in base al modello specifico del settore e non già al quadro più generale.

## 2 Analisi

Il Gruppo di lavoro prende atto dell'entità del lavoro svolto dagli autori del quadro proposto e ne condivide i principali obiettivi, evidenziati nelle sezioni introduttive.

Benché l'impostazione generale del quadro non presenti problemi particolari, il Gruppo di lavoro ha individuato, ed espone di seguito, tre importanti motivi di preoccupazione a livello di contenuto e alcune osservazioni.

### 2.1 Valutazione dei rischi

La sezione introduttiva del quadro proposto dichiara senza ambiguità che il processo di valutazione d'impatto sulla protezione della vita privata e dei dati è concepito per individuare i rischi per la vita privata connessi a un'applicazione RFID e valutare le misure prese per farvi fronte. **Tuttavia, questo principio centrale del processo di valutazione dell'impatto sulla privacy non figura nel contenuto del quadro proposto.**

Infatti, sebbene il quadro proposto contenga riferimenti sparsi alla valutazione dei rischi (soprattutto nelle parti introduttive) nessuna sezione impone espressamente al gestore RFID di *individuare i rischi per la vita privata connessi a un'applicazione RFID*. Ne consegue che non è possibile *valutare le misure prese per farvi fronte*. Il quadro proposto obbliga infatti il gestore RFID solamente a elencare i vari

controlli e salvaguardie messi a punto per proteggere la vita privata e i dati personali nell'applicazione RFID. Non si può ritenere tale obbligo un mezzo soddisfacente che garantisca al gestore RFID o all'autorità competente la ragionevole sicurezza circa l'adeguatezza o proporzionalità ai rischi delle misure proposte, in quanto tali rischi non sono stati precedentemente individuati.

Il Gruppo di lavoro si rammarica profondamente che gli autori del quadro proposto non abbiano affrontato questo aspetto.

Un quadro per la realizzazione di valutazioni d'impatto sulla protezione dei dati personali e della vita privata dovrebbe per definizione proporre una metodologia generale che preveda, quale elemento essenziale, una fase di valutazione dei rischi. L'industria RFID senza dubbio esegue già valutazioni dei rischi nell'ambito dell'approccio metodologico nel contesto della gestione della sicurezza delle informazioni, di cui alla norma ISO/IEC 27005<sup>8</sup> e altre norme nazionali o internazionali. Il Gruppo di lavoro è convinto che l'industria RFID potrebbe basarsi su questo insieme di competenze acquisite nella gestione tradizionale della sicurezza delle informazioni per arricchire il quadro con un adeguato approccio della valutazione dei rischi. Ciò inoltre inciderebbe su altri elementi specifici del quadro proposto, come si evidenzia in particolare nei punti 2.2, 2.3 e 2.4 del presente parere.

Inoltre, nel considerando 17 della raccomandazione RFID si legge che lo sviluppo di un siffatto 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)"*. Tale considerando legittima gli autori del quadro proposto a considerare attentamente il recedente parere dell'ENISA sul quadro per la valutazione dell'impatto sulla privacy<sup>9</sup> e a chiedere ulteriori orientamenti all'agenzia UE in merito all'attuazione di un approccio della valutazione dei rischi nel contesto delle applicazioni RFID. L'ENISA ha specificamente assunto<sup>10</sup> l'incarico di individuare e valutare i rischi emergenti e futuri di un particolare scenario IoT/RFID, segnatamente nel contesto del ruolo dell'ENISA specificato nella comunicazione della Commissione *"L'internet degli oggetti: un piano d'azione per l'Europa"*<sup>11</sup>. **Il Gruppo di lavoro incoraggia vivamente l'industria a cogliere questa opportunità.**

## **2.2 Etichette portate da persone**

Uno dei tre principali motivi di preoccupazione per la vita privata evidenziati nel *documento di lavoro sulle questioni relative alla protezione dei dati collegate alla tecnologia RFID* (WP 105)<sup>12</sup> deriva dagli usi della tecnologia RFID che implicano il tracciamento delle persone e l'accesso ai dati personali. Gli articoli muniti di etichette portati da una persona contengono infatti identificatori unici che si possono leggere a distanza. A loro volta tali identificatori unici potrebbero essere usati per riconoscere quella

---

<sup>8</sup> Cfr. ISO/IEC 27001:2005, Tecnologie dell'informazione – Tecniche di sicurezza – Sistemi di gestione della sicurezza delle informazioni – Requisiti

<sup>9</sup> Parere ENISA sulla proposta dell'industria relativa a un quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID, luglio 2010, <http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia> (in inglese).

<sup>10</sup> Si veda, ad esempio, la relazione ENISA report *"Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology"*.

<sup>11</sup> Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - L'internet degli oggetti: un piano d'azione per l'Europa, COM(2009) 278, Bruxelles, 18.6.2009.

<sup>12</sup> Cfr. nota 2.

determinata persona nel tempo, rendendola così "identificabile". Sebbene ciò sia auspicabile in alcuni casi, specie quando l'articolo munito di etichetta è appositamente concepito come meccanismo di controllo (ad esempio un badge), in altri casi può consentire a terzi di tracciare<sup>13</sup> una persona a sua insaputa. Come si evidenzia nel parere 4/2007 sul concetto di dati personali (WP 136)<sup>14</sup>, l'identificatore unico associato a una persona rientra nella definizione di "dati personali" di cui alla direttiva 95/46/CE, indipendentemente dal fatto che l'"identità sociale" (nome, indirizzo, ecc.) della persona rimanga ignota (ossia la persona è "identificabile" ma non necessariamente "identificata").

Inoltre, il numero unico inserito nell'etichetta può servire anche per identificare da lontano la natura degli articoli portati da una persona, e rivelare quindi informazioni sullo status sociale, sulla salute o altro. Pertanto, anche quando l'etichetta contiene solo un numero che è unico in un particolare contesto, senza dati personali aggiuntivi, se l'etichetta è destinata a essere portata da persone occorre prestare particolare attenzione ai rischi potenziali per la vita privata e la sicurezza.

Il Gruppo di lavoro si compiace che l'industria abbia riconosciuto questo problema nel quadro per la valutazione dell'impatto sulla privacy rendendo obbligatoria la valutazione quando *"le etichette poste sugli articoli sono destinate ad essere portate da persone"* ("applicazioni di livello 1").

Purtroppo, malgrado la premessa **il quadro proposto** non risponde a questa preoccupazione e **omette di invitare espressamente il gestore RFID a valutare gli aspetti di protezione della vita privata e dei dati che potrebbero dare adito a problemi quando sono le persone a portare le etichette nella vita di tutti i giorni.** Non è sufficiente esaminare se *"tramite l'applicazione RFID sarà controllato dove si trova il singolo o l'utente"*<sup>15</sup>. È altresì fondamentale **analizzare il rischio di un controllo non autorizzato al di fuori del perimetro dell'applicazione.** Il quadro omette inoltre di descrivere le misure prese per far fronte a tali rischi. **Il Gruppo di lavoro sollecita l'industria ad affrontare tale questione a tutto campo, menzionandola chiaramente nel quadro nell'ambito di un approccio rivisto alla valutazione dei rischi.**

### **2.3 RFID nel settore del commercio al dettaglio**

Uno dei settori chiave di applicazione della tecnologia RFID in cui le etichette potrebbero essere portate da persone è il settore del commercio al dettaglio. La raccomandazione RFID riconosce il carattere critico di tale settore e vi dedica punti specifici.

Il punto 11 della raccomandazione RFID precisa specificamente che *"i commercianti al dettaglio dovrebbero disattivare o rimuovere nel punto di vendita le etichette usate nelle loro applicazioni, a meno che i consumatori [...] acconsentano a mantenere le etichette operative"*.

Il punto 12 introduce una deroga a tale regola, disponendo che *"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"*

<sup>13</sup> Cfr. gli esempi di cui al WP 105, punto 3.3.

<sup>14</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp136\\_it.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_it.pdf)

<sup>15</sup> Sezione 2.3.4 del quadro proposto.

personali". Ciò significa che di default si deve procedere alla disattivazione nel punto di vendita, salvo che la valutazione dell'impatto sulla privacy giunga a una conclusione diversa.

Tuttavia, la sezione D del quadro proposto contempla solo due conclusioni possibili per la relazione sulla valutazione: l'applicazione RFID "è pronta per essere introdotta" oppure "non è pronta per essere introdotta", senza possibilità per il gestore RFID di formulare una conclusione sull'uso delle etichette al di fuori del punto di vendita nelle applicazioni del commercio al dettaglio, come richiesto dalla raccomandazione RFID. Il Gruppo di lavoro rileva che certe applicazioni possono giustificare o richiedere che, per finalità specifiche, alcune etichette rimangano attive al di fuori del punto di vendita nelle applicazioni del commercio al dettaglio. L'assenza di considerazioni di questo tipo nel quadro proposto sembra però implicare che, fuori dai punti di vendita, tutte le etichette saranno disattivate.

Più in generale, il Gruppo di lavoro osserva che la scelta binaria prevista nella sezione D del quadro sembra inutilmente restrittiva per i gestori RFID e l'industria RFID nel suo complesso. Si potrebbe ritenere che alcune applicazioni siano "pronte per essere introdotte a determinate condizioni" da specificarsi nella conclusione della relazione sulla valutazione.

**Il Gruppo di lavoro invita gli autori del quadro proposto a chiarire la questione della disattivazione delle etichette nel settore del commercio al dettaglio.** Il quadro proposto deve espressamente fare obbligo al gestore RFID di trattare il punto 12 della raccomandazione RFID nella relazione sulla valutazione (per le applicazioni del commercio al dettaglio). **Più in generale, l'approccio rivisto della valutazione dei rischi dovrebbe fornire gli strumenti giusti per giungere a una conclusione sulle condizioni o sull'introduzione di un'applicazione RFID.**

## **2.4 Altre osservazioni**

Come evidenziato al punto 2.2, se l'etichetta è portata da una persona (utente o singolo) e contiene un ID unico<sup>16</sup>, per definizione essa contiene dati personali. A rigor di termini, le definizioni di "applicazioni di livello 1" e "applicazioni di livello 0" di cui alla sezione 1.4 presentano quindi una contraddizione: nella maggior parte degli scenari non è possibile affermare che l'applicazione RFID *non* tratta dati personali se le etichette sono portate da singoli o utenti. Pertanto, in base a tali definizioni, la maggior parte delle applicazioni sarebbe di livello 2. **Si avrebbero applicazioni di livello 0 o di livello 1 solo nei rari casi in cui le etichette sono portate da persone e non contengono un numero unico.**

Il Gruppo di lavoro presume che gli autori del quadro proposto non intendessero attribuire un campo di applicazione così limitato alle applicazioni di livello 0 e di livello 1, e che le relative definizioni intendessero comprendere le applicazioni che trattano solo un tipo di dati personali, segnatamente l'ID unica dell'etichetta. Tutte le definizioni dei livelli potrebbero facilmente essere chiarite per eliminare ogni ambiguità. In ogni caso, la definizione corretta di una metodologia basata sulla valutazione dei rischi potrebbe comportare anche una riformulazione di tali definizioni.

Il Gruppo di lavoro osserva che il quadro fa riferimento a etichette "*possedute*" da utenti o singoli. Tale termine è troppo restrittivo e dovrebbe essere sostituito dal termine "portate", che copre in modo molto più appropriato gli scenari di rischio in questione.

---

<sup>16</sup> Facciamo generico riferimento all'"etichetta ID" per indicare qualunque numero (o numero di serie) identificativo unico a cui si può accedere nell'etichetta RFID e che consente di caratterizzare in modo unico un'etichetta RFID in un determinato contesto.

Il Gruppo di lavoro ritiene che il processo di valutazione dell'impatto sulla privacy proposto nel quadro dovrebbe includere una fase di consultazione delle parti interessate, ossia di quelle parti (gruppi, sindacati, associazioni) che possono avere un interesse nell'applicazione RFID, e di scambiare idee, proposte e miglioramenti per introdurre l'applicazione in modo aperto e rispettoso della vita privata, a vantaggio sia del gestore RFID sia degli utenti o singoli interessati. Tale fase di consultazione contribuisce chiaramente alle “*informazioni e trasparenza sull'uso della RFID*” e alle “*attività di sensibilizzazione*” di cui alla raccomandazione RFID.

Il Gruppo di lavoro sottolinea inoltre che sono necessarie condizioni specifiche per trattare in modo lecito e sicuro categorie particolari di dati<sup>17</sup>. Il quadro dovrebbe fornire al gestore RFID orientamenti più decisi sulle questioni specifiche relative al trattamento di categorie particolari di dati (detti anche “dati sensibili”). Il processo di valutazione dei rischi dovrebbe inoltre includere sempre l'individuazione dell'uso di tali categorie.

Il quadro dovrebbe anche fornire ai gestori RFID orientamenti sulle condizioni e sul momento più opportuno per eseguire la valutazione dell'impatto sulla privacy nel ciclo di sviluppo di un prodotto RFID, in modo da incoraggiare realmente il principio della “*sicurezza e tutela della vita privata garantiti fin dalla fase di progettazione*” sostenuto dalla raccomandazione.

### 3 Conclusione

Alla luce dei problemi evidenziati nel presente parere, in particolare l'assenza nel quadro proposto di un approccio chiaro e globale di valutazione dei rischi per la protezione della vita privata e dei dati, **il Gruppo di lavoro non approva il documento proposto nella versione attuale.**

Va rilevato che l'inclusione di un corretto processo di valutazione dei rischi può chiaramente agevolare la soluzione di molti degli altri aspetti problematici individuati nel presente parere. Infatti, se il gestore RFID fosse tenuto a eseguire una valutazione dei rischi individuerebbe in particolare i rischi connessi al controllo non autorizzato delle etichette RFID portate da persone. Inoltre, nel settore del commercio al dettaglio, la valutazione dei rischi potrebbe aiutare a presentare un esempio chiaro di come determinate etichette RFID (usate in un'applicazione specifica) che “*resteranno operative al di fuori del punto di vendita non rappresentano una probabile minaccia alla vita privata o alla protezione dei dati personali*”.

Il Gruppo di lavoro è convinto che l'industria sia in grado di proporre un quadro migliore che tenga conto delle osservazioni formulate nel presente parere, e si impegna a seguire le vie necessarie per migliorare ulteriormente il quadro proposto e approvarlo rapidamente.

Fatto a Bruxelles, il 13 luglio 2010.

*Per il Gruppo di lavoro*  
*Il Presidente*  
*Jacob KOHNSTAMM*

---

<sup>17</sup> Articolo 8 della direttiva 95/46/EC.