PUBBLICAZIONE SEMESTRALE
ANNO X - N. 1 GENNAIO-GIUGNO 2005

ISSN 1127-2872

Contratto e impresa / Europa

1

anno decimo

a cura di

F. Galgano e M. Bin

Diritto civile europeo: problemi generali; *acquis communautaire*

Impresa: principio di "precauzione"; prospetti informativi; *sicar* lussemburghese; nuova normativa francese

Concorrenza: la nuova procedura comunitaria; *gambling*

Proprietà industriale: *domain name*; *industrial design*

Contratti: vendita di beni di consumo in Francia; contratti su internet

Riconoscimento ed esecuzione dei lodi stranieri

Diritto comunitario: mediazione e conciliazione; medicinali generici

Indicatori a radiofrequenza

La legge comunitaria (2004)

2005

CEDAM

Identificatori a radiofrequenza (RFID): si delineano le prime linee guida comunitarie

Negli ultimi anni il settore delle tecnologie digitali applicate alla produzione ed alla distribuzione si è caratterizzato per la comparsa e la rapida diffusione dei sistemi di identificazione a radiofrequenza, capaci di rivoluzionare non solo la gestione del settore logistico, ma anche il *direct-marketing*, la domotica, i sistemi di sicurezza e quant'altro. L'ambito applicativo dei dispositivi di identificazione a radiofrequenza o RFID (acronimo di *Radio-Frequency Identification Devices*) è infatti in continua espansione, sebbene agli occhi del comune cittadino esso spesso risulti invisibile.

Dal punto di vista strutturale gli identificatori a radio frequenza, anche noti come *e-tag* (*electronic-tag*), consistono in minuscole etichette elettroniche (1) capaci di memorizzare e trasmettere dati ad appositi lettori mediante l'impiego di onde radio (2).

Il superamento dell'iniziale «fase sperimentale» dell'applicazione di tali dispositivi si è avuta nel corso dell'ultimo anno e mezzo (3): la progressiva diffusione delle *e-tag* ne ha infatti favorito la diminuzione dei costi di produzione (4) e, contemporaneamente, ha consentito di potenziare la ricerca sotto i diversi aspetti della miniaturizzazione e delle capacità operative. Pare dunque destinata ad avverarsi in tempi brevi la «profezia»

---

(1) La miniaturizzazione dei dispositivi RFID è in continuo avanzamento e, attualmente, si sono raggiunte grandezze dell'ordine di un terzo di millimetro, tuttavia la maggior parte delle *e-tag* applicate sui prodotti in commercio hanno dimensioni che si aggirano sui due centimetri di diametro.

(2) Occorre al riguardo distinguere fra dispositivi RFID «passivi», in grado di inviare dati solo se appositamente sollecitati dal lettore (che, mediante l'emissione di onde elettromagnetiche, fornisce loro l'energia necessaria alla trasmissione) e dotati di un ridotto raggio d'azione, e «attivi», capaci di operare autonomamente, inviando informazioni e creando reti comunicative con altri dispositivi.

(3) Tra i primi gruppi ad impiegare le tecnologie a radiofrequenza in via sperimentale si possono ricordare, a titolo d'esempio, Wal-Mart, Tesco, Metro, Gilette, Benetton.

(4) Sul rapporto fra diminuzione dei costi di produzione e diffusione degli RFID cfr. gli studi di WEIS, *Security and Privacy in Radio-Frequency Identification Devices*, Massachusetts Institute of Technology, Cambridge (Massachusetts)-London, 2003, p. 14, nonché SARMA, *Towards the five-cent tag. Technical Report MIT-AUTOID-WH-006*, MIT Auto-ID Center, 2001 e SCHARFELD, *An Analysis of the fundamental Constraints on low Cost Passive Radio-Frequency Identification System Design*, Massachusetts Institute of Technology, Cambridge (Massachusetts)-London, 2001.

dell'Auto-ID Center, ove gli studi sui dispositivi RFID hanno avuto inizio (5), secondo cui si arriverà a creare «un'infrastruttura globale... che consentirà ai computer di identificare istantaneamente qualsiasi oggetto in qualsiasi parte del mondo» (6).

Non possono dunque sfuggire le evidenti implicazioni in termini di trattamento dei dati personali e di controllo sociale che l'impiego di simili applicazioni comporta, sebbene allo stato attuale tale profilo appaia poco considerato negli studi di settore (7).

In proposito occorre evitare di incorrere in facili allarmismi o in tentazioni «tecnoclastiche», preannunciando (secondo un ricorrente adagio in tema di dati personali) l'ennesimo avvento del Grande Fratello di orwelliana memoria o, se si preferisce il genere, scenari da *Minority Report* (8). La tecnologia RFID, come ogni altra, offre infatti un immenso potenziale che sta solo all'uomo scegliere di sfruttare in maniera consapevole e fruttuosa oppure in maniera scellerata e lesiva degli altrui diritti. In specie sono evidenti i vantaggi derivanti dalle applicazioni degli identificatori a radiofrequenza in molteplici campi, sia attinenti ai processi produttivi che

(5) L'Auto-ID Center è stato creato nel 1999 da una collaborazione fra il Massachusetts Institute of Technology, l'Università di Cambridge e l'Università di Adelaide ed un gruppo di oltre 50 multinazionali (tra cui Coca-Cola, Gilette, Johnson & Johnson, Pfizer, Procter & Gamble, Unilever, UPS e Wal-Mart). Il centro ha tuttavia cessato la propria attività nell'ottobre 2003 a seguito della diffusione di alcuni documenti riservati da cui emergeva l'intento di occultare, o quanto meno sottostimare, i rischi per la tutela della *privacy* connessi alla diffusione delle *e-tag*, che stavano preoccupando l'opinione pubblica (specie quella statunitense). L'attività di ricerca e l'applicazione industriale hanno così proseguito separatamente il proprio sviluppo, l'una nell'ambito universitario del neonato Auto-ID Labs (a cui aderiscono il Massachusetts Institute of Technology e le università di Cambridge, Adelaide, Keio, Fudan e St. Gallen) e l'altra all'interno dell'EPCglobal Inc.

(6) La frase è tratta dal documento di presentazione del progetto dell'Auto-ID Center, intitolato *La nuova rete. Identificazione automatica di qualsiasi oggetto in qualsiasi luogo*, che era consultabile sul sito di tale istituto di ricerca www.autoidcenter.org (visitato il 15.04.03) fino alla sua chiusura.

(7) Per un primo esame delle implicazioni giuridiche connesse alla diffusione dei dispositivi RFID, svolto su queste pagine, sia consentito rinviare a MANTELERO, *Identificatori a radiofrequenza (rfid) e controllo capillare dei dati personali: il rischio di un «mondo nuovo» per il consumatore ?*, in *questa rivista,* 2004, p. 1 ss., ove più ampi riferimenti alle caratteristiche applicative delle *e-tag* ed alla loro compatibilità con le disposizioni di cui al d. lgs. 196/03.

(8) In questa trasposizione cinematografica (USA 2002, regia di Steven Spielberg) del noto racconto di Philip K. Dick, viene evocato un futuro in cui ciascun soggetto può essere controllato ed individuato, in cui i manifesti pubblicitari chiamano per nome le singole persone, invitandole ad acquistare un determinato prodotto.

ne anche nelle ipotesi in cui il dispositivo RFID non porti all'identificazione della persona, ma solo all'individuazione della stessa quale identità innominata isolabile dal resto dei consociati in quanto centro di riferimento di una pluralità di beni contrassegnati da *e-tag*. Viene dunque considerata attività di profilazione anche quella che non porta all'abbinamento finale fra cosa e persona, come accade ad esempio nel momento in cui il cliente paga con la propria carta di credito, ma che consente comunque di trattare uno specifico profilo come un *unicum* a sé stante, quale aggregato di beni e preferenze determinate ([17]), conseguentemente suscettibile di sollecitazioni mirate e di tracciatura delle abitudini commerciali, in maniera analoga a quanto avviene *on-line* mediante l'impiego dei *cookie*.

L'applicabilità della normativa in materia di dati personali comporta la necessità di acquisire, salvo i casi di deroga, il consenso informato del soggetto che entra nella disponibilità di un bene contrassegnato da un dispositivo RFID, a tal fine dovrà essere in particolare indicata la capacità del dispositivo di operare indipendentemente da qualsiasi comportamento attivo posto in essere dall'utente, nonché specificata la tipologia di *e-tag* utilizzata ([18]), se passiva o attiva ([19]). La natura «persistente» del marcatore elettronico implica inoltre l'informazione circa le modalità mediante le quali lo stesso può essere disattivato temporaneamente ([20])

([17]) Tecnicamente ciò è possibile proprio grazie al carattere persistente dei marcatori, siano essi dispositivi RFID se applicati nel mondo «reale» o *cookies* se operanti in quello «virtuale» di *internet*. Entrambi i dispositivi, grazie alla loro capacità di rimanere in maniera persistente abbinati ad un soggetto (chi detiene i beni su cui l'*e-tag* è posta o chi adopera per «navigare» sul *web* il computer nel cui *hard disk* è stato memorizzato il *cookie*) permettono a chiunque disponga di un rilevatore atto a percepire la presenza del marcatore di riconoscere il soggetto «marcato» ogni qualvolta gli si presenti; in tal maniera è possibile dunque identificare indirettamente lo stesso ai sensi dell'art. 2, lett. a, dir. 95/46/CE e dell'art. 4, c. 1, lett. b, d. lgs. 196/03. In ragione dell'economicità del presente contributo sia consentito rinviare alle considerazioni espresse circa il rapporto fra profilazione, anonimato ed impiego di «marcatori», in MANTELERO, *Attività di impresa in Internet e tutela della persona*, Padova, 2004, p. 159 ss.

([18]) Al fine di semplificare la comunicazione della presenza di un dispositivo RFID, in previsione della diffusione su grande scala di tale tecnologia ed in considerazione della natura anche minuscola degli oggetti contrassegnati e dei dispositivi medesimi, il documento redatto dall'Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, cit., p. 14, suggerisce anche il ricorso all'apposizione sui beni di un logo *standard*. Cfr. già in tal senso WEIS, *op. cit.*, p. 59.

([19]) Sulle diverse tipologie di identificatori a radiofrequenza cfr. *supra* nota 2 e, più diffusamente, WEIS, *op. cit.*, p. 17 ss.

([20]) Un simile risultato può essere conseguito impedendo la trasmissione radio con il dispositivo RFID, mediante il ricorso a strutture isolanti (involucri) o tali da ingenerare in

o in via definitiva (21). Dovrebbero infine essere rese disponibili apposite apparecchiature che consentano di verificare l'eventuale presenza di *e-tag* e la loro attività, nel caso in cui non vengano fornite le dovute indicazioni a riguardo (22).

Mentre le linee guida ora esaminate, sebbene attualmente non seguite da molte imprese, costituiscono la ricezione degli orientamenti emersi a livello internazionale sia fra gli operatori del diritto che fra i diversi tecnici che si sono occupati della realizzazione e dello sviluppo dei dispositivi RFID (23) e potrebbero quindi non riscontrare eccessive diffi-

---

terferenze elettromagnetiche. Queste soluzioni presentano tuttavia alcuni effetti indesiderati: le prime possono risultare incompatibili con le dimensioni del bene su cui l'*e-tag* è posta, mentre le seconde comportano effetti di disturbo generalizzati, dunque rispetto a qualsiasi dispositivo RFID presente e non solo a quello che si vuole inibire. Cfr. a riguardo JUELS-RIVERST-SZYDLO, *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*, 2003, p. 4, in http://theory.lcs.mit.edu (visitato il 15.03.04). Per tali ragioni pare più efficiente il ricorso a metodologie in cui l'attivazione e la disattivazione del dispositivo dipendano direttamente dal contenuto informativo dello stesso, ad esempio variando i numeri di serie in maniera tale da rendere l'etichetta elettronica non più leggibile dai ricevitori e, nel contempo, dotando il consumatore di un dispositivo in grado di realizzare l'operazione inversa al fine di riattivare l'*e-tag*, come suggerito da JUELS-RIVERST-SZYDLO, *op. cit.*, p. 7 ss.

(21) Si tratta del cosiddetto «kill approach», consistente nell'arrecare un danno irreparabile ai componenti dell'*e-tag*, cfr. JUELS-RIVERST-SZYDLO, *op. cit.*, p. 3. Il diritto di disabilitare ogni dispositivo RFID posto sui beni acquistati è stato affermato nella Risoluzione sugli identificatori a radiofrequenza adottata a Sydney il 20 novembre 2003, www.privacyconference2003.org (visitato il 23.03.05). In tal senso si erano anche pronunciati alcuni dei progettisti degli identificatori a radiofrequenza, i quali avevano ideato dei dispositivi tecnici volti alla disattivazione o alla distruzione dell'*e-tag*, cfr. GARFINKEL, *An RFID Bill of Rights*, in *Technology Review*, Oct. 2002, p. 35. Si vedano inoltre le *Guidelines on EPC for Consumer Products* formulate dall'EPCglobal Inc., consultabili al sito www.epcglobalinc.org (visitato il 23.03.05). Con riguardo ai diversi strumenti tecnici utilizzabili ai fini di disattivare temporaneamente o in via definitiva i dispositivi RFID, nel documento redatto dall'Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, cit., p. 15 ss., vengono indicate alcune modalità che sostanzialmente riprendono le soluzioni esistenti allo stato della tecnica menzionate in questa e nella precedente nota.

(22) Tale eventualità non risulta affatto remota, trattandosi di dispositivi nano-tecnologici che possono raggiungere dimensioni anche inferiori al millimetro. Al riguardo potrebbe essere utile installare, all'interno dei punti di vendita o in luoghi pubblici definiti, appositi lettori mediante i quali ciascuno possa verificare l'emissione di onde elettromagnetiche e così vagliare la presenza e l'eventuale attività dell'identificatore a radiofrequenza.

(23) Cfr., fra gli altri, WEIS, *op. cit.*, *passim*; JUELS-RIVERST-SZYDLO, *op. cit.*, *passim*; GARFINKEL, *op. cit.*, *passim*.

coltà d'adozione, più controversa pare l'indicazione emergente a livello comunitario con riguardo alla sicurezza dei dati personali. Nel documento approvato viene infatti indicato il ricorso alla crittografia come soluzione preferenziale per consentire la protezione delle informazioni da accessi indebiti (24). L'adozione di tale sistema di protezione, come sottolineato dagli studi tecnici in materia (25), presenta tuttavia dei costi difficilmente compatibili con il basso prezzo di mercato che devono necessariamente avere gli identificatori a radiofrequenza per essere impiegati su scala industriale (26), a meno di trasferire il processo di criptazione e decriptazione dall'*e-tag* al lettore (27).

Con riguardo agli orientamenti emersi a livello comunitario va osservato come alcuni tratti salienti degli stessi, specie per quanto concerne gli obblighi informativi circa la presenza e la natura dei dispositivi RFID, siano riscontrabili anche in differenti contesti giuridici. Così, nonostante le divergenze in materia di dati personali presenti fra Unione Europea e Stati Uniti, sono state recentemente avanzate specifiche iniziative legislative

(24) Cfr. Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, cit., p. 17: «The type of technical means will depend on the nature of the data. As further illustrated below, most of the time, these tags could require the *encryption* of the data and the authentication of the reader to prevent third parties provided with readers from reading the information».

(25) Cfr. in tal senso JUELS-RIVERST-SZYDLO, *op. cit.*, p. 5 e JULES-PAPPU, *Squealing Euros: Privacy protection in RFID-enabled banknotes*, 2003, p. 3, pubblicato sul sito www.rsasecurity.com (visitato il 15.03.04).

(26) Tale profilo problematico non pare sfuggire nemmeno agli autori dell'Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, cit., p. 17, in cui conclusivamente si legge: «There already exist publication that indicate that symmetric algorithms (such as AES) are suitable for RFID tags. The problem of using symmetric authentication algorithms is that the key establishment and the key management is complex. Asymmetric methods avoid those problems, but are more expensive than symmetric ones». In specie viene richiamato il seguente studio: FELDHOFER-DOMINIKUS-WOLKERSTORFER, *Strong Authentication for RFID Systems using the AES Algorithm*, in *Lecture Notes in Computer Science (LNCS)*, vol. 3156, Springer Verlag, 2004, p. 357 ss. Cfr. altresì a riguardo AIGNER-FELDHOFER, *Secure Symmetric Authentication for RFID Tags*, 2005, pubblicato sul sito http://tcmc.tugraz.at/tcmc2005/PDF/20050228-IAIK-SecureAuthentication.pdf (visitato il 28.03.05). Tra i recenti contribuiti in tema di sicurezza delle informazioni memorizzate nei dispositivi RFID ed impiego di tecniche crittografiche si vedano: BONO-GREEN-STUBBLEFIELD-JUELS-RUBIN-SZYDLO, *Security Analysis of a Cryptographically-Enabled RFID Device* e JUELS, *Minimalist Cryptography for Low-Cost RFID Tags*, entrambi pubblicati sul sito www. rsasecurity.com (visitato il 28.03.05).

(27) Cfr. GOLLE-JAKOBSSON-JULES-SYVERSON, *Universal re-encryption for mixnets*, 2004, pubblicato sul sito www.rsasecurity.com (visitato il 31.03.04).

in alcuni stati degli USA ([28]) che manifestano diverse affinità con gli orientamenti delineati dalle linee guida comunitarie, dimostrando come il medesimo sostrato tecnologico dei problemi giuridici da affrontare favorisca necessariamente, nel campo delle *e-tag*, come già in quello di internet, una spontanea convergenza fra le soluzioni adottate nei vari ordinamenti.

In ambito nazionale si segnala infine il recente intervento del Garante per la protezione dei dati personali ([29]) che, in accordo con le indicazioni emerse a livello comunitario e con analoga finalità « di consentire ad operatori e produttori di predisporre dispositivi offerti in conformità alla normativa in materia di tutela dei dati personali », ha prescritto specifiche misure da adottarsi nell'impiego delle tecniche di identificazione a radiofrequenza ([30]).

Nel provvedimento del Garante, oltre a ribadire la necessità di adoperare tale nuova tecnologia in maniera coerente con i principi generali fissati dal d. lgs. 196/03 ([31]), si precisa che, nel caso di dispositivi applicati su beni posti in vendita, le *e-tag* dovranno essere disattivate all'atto dell'acquisto, salvo che il perdurare della funzionalità delle stesse non sia necessario per fornire un servizio specificamente e liberamente richiesto dall'acquirente ([32]). Viene poi previsto l'obbligo di informativa non solo rela-

([28]) Proposte di regolamentazione dei dispositivi a radiofrequenza, sostanzialmente ispirate alla tutela dei diritti dei consumatori, sono state avanzate, seppur senza successo, nel 2004 in California (SB 1834), Missouri (S.B. 867), Utah (HB 251) e New Mexico (HB 215).

([29]) Cfr. Garante per la protezione dei dati personali, provvedimento a carattere generale del 9 marzo 2005, pubblicato sul sito ufficiale dell'Autorità www.garanteprivacy.it. La redazione del provvedimento è stata preceduta da una consultazione pubblica riguardante i dispositivi RFID (cfr. *Newsletter*, notiziario settimanale del Garante per la protezione dei dati personali, n. 239 del 27 dicembre 2004-2 gennaio 2005) onde acquisire ulteriori elementi di valutazione dalle osservazioni provenienti dagli operatori di settore e dai comuni cittadini. Attenzione per il tema era già stata mostrata in precedenza dall'Autorità Garante: cfr. *Newsletter*, notiziario settimanale del Garante per la protezione dei dati personali, n. 172 del 26 maggio 2003, n. 193 del 24 novembre 2003, n. 196 del 5 gennaio 2004, pubblicati sul sito ufficiale dell'Autorità www.garanteprivacy.

([30]) In specie, con riferimento all'esercizio dei diritti di cui all'art. 7 del d. lgs. 196/03, nel provvedimento adottato dal Garante per la protezione dei dati personali si legge: « Già nella fase di progettazione delle tecnologie, i produttori di sistemi *RFID* dovrebbero opportunamente predisporre modalità idonee a garantire agli interessati un agevole esercizio dei diritti ».

([31]) Vengono al riguardo esplicitamente richiamati gli artt. 3 ed 11, d. lgs. 196/03.

([32]) In proposito, nel provvedimento del 9 marzo 2005, il Garante ha precisato che « fermo restando... che non è di regola lecita l'installazione di etichette *RFID* destinate a rimanere attive anche oltre la barriera-cassa dell'esercizio commerciale in cui sono utilizzate, tale ipotetico impiego, ove lecito, presuppone comunque il necessario consenso dell'interessato, a meno che possa operare un altro presupposto equipollente del trattamento ».

tivamente agli identificatori a radiofrequenza, ma anche con riferimento ai dispositivi di lettura degli stessi, qualora essi siano presenti ed attivi in una determinata area (33).

ALESSANDRO MANTELERO

(33) Si legge nel provvedimento citato: «deve essere segnalata mediante informativa l'esistenza di lettori in grado di 'attivare' l'etichetta (lettori i quali possono comunque essere posti in essere solo in quanto strettamente necessari in rapporto alla finalità del trattamento)».