Fidelizzazione, profilazione e privacy della clientela in ambito commerciale: breve disamina degli orientamenti del Garante per la protezione dei dati personali

Giuseppe Staglianò

Sommario: 1. Il progresso tecnologico e le nuove frontiere della riservatezza; 2. Opportunità di mercato, risorse aziendali e nuove fonti normative; 3. I programmi di fidelizzazione e la profilazione nella grande distribuzione; 4. La tecnologia *Rfid*: le c.d. "etichette intelligenti".

1. Il progresso tecnologico e le nuove frontiere della riservatezza.

Tra le questioni più importanti di cui il Garante è chiamato costantemente ad occuparsi, particolare interesse rivestono quelle relative alla tutela dei dati personali acquisiti ed utilizzati da coloro che, a vario titolo, operano nell'ambito del c.d. *direct marketing*, espressione nella quale, in linea di massima, si è soliti ricomprendere l'attività d'invio di materiale pubblicitario, l'espletamento di ricerche di mercato, la comunicazione commerciale interattiva e la vendita diretta.

Si tratta di un settore oramai intimamente connesso a quello della comunicazione telematica, il quale è caratterizzato da un continuo sviluppo tecnologico e, quindi, dall'incessante formulazione di nuove offerte di servizi accessibili al pubblico; ad esso si accompagna, in modo speculare, sia nell'ambito della telefonia, sia in quello della rete

Internet, un costante incremento del numero degli utenti, con un aumento esponenziale delle informazioni trasmesse. Di ciò si sono dimostrati consapevoli il Parlamento ed il Consiglio europeo che, con la direttiva 2002/58/CE[1] (che ha modificato la precedente direttiva 97/66/CE), hanno dettato appositi principi sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche (G.U.C.E., n. L 201 del 31 luglio 2002). In particolare, la direttiva in questione, nell'intento di predisporre un complesso di regole valido ed applicabile a tutte le forme di comunicazione elettronica effettuate per via telefonica, attraverso la rete Internet o mediante altri mezzi, è stata emanata con il dichiarato fine di adeguare la disciplina sulla tutela dei dati personali alle attuali opportunità dei mercati e alle possibilità offerte dalle moderne tecnologie dei servizi di comunicazione elettronica.

2. Opportunità di mercato, risorse aziendali e nuove fonti normative.

Di questa realtà, comunque, hanno dimostrato di avere già piena coscienza gli utenti ed i consumatori italiani, i quali, in più occasioni, hanno lamentato fastidiose intrusioni nella loro vita privata connesse

[1] L'adozione della direttiva n. 2002/58/CE è stata determinata dalle novità tecnologiche introdotte nei servizi di comunicazione elettronica e dalle conseguenti ricadute sui singoli settori di mercato, che hanno costretto il Parlamento ed il Consiglio europeo a predisporre norme per consentire agli utenti ed ai consumatori di usufruire di un'adeguata forma di tutela dei dati e della vita privata, a prescindere dal tipo di tecnologia – digitale o analogica – concretamente impiegato (in proposito vedi il considerando n. 4).
La direttiva in questione, peraltro, faceva parte di un complesso di norme teso a disciplinare compiutamente il settore delle comunicazioni elettroniche ed a sostituire la precedente normativa in materia di telecomunicazioni. Di tale complesso facevano parte altre quattro direttive (n. 2002/21/CE, concernente il quadro generale; n. 2002/19/CE, sull'accesso e la interconnessione; n. 2002/20/CE, in tema di autorizzazioni e licenze; n. 2002/22/CE, sul servizio universale), che hanno trovato attuazione con il Codice delle comunicazioni elettroniche (d. lg. 1 agosto 2003, n. 259).

all'impiego, da parte delle aziende, di nuove tecnologie e di moderne strategie, atte a commercializzare, secondo formule più aggressive, i prodotti ed i servizi offerti.

Analogamente, molti fornitori di servizi per via telematica, dimostrando di considerare l'introduzione di misure di tutela della vita privata come strumento utile per rafforzare un rapporto di fiducia con gli utenti e non come un mero dovere legale, hanno formulato al Garante una serie di richieste di tipo preventivo, per evitare di arrecare possibili lesioni ai diritti fondamentali dei propri clienti e, al contempo, per acquisire una maggiore qualificazione sul piano imprenditoriale che, di fatto, si è tradotta in un incremento delle risorse aziendali.

Ciò premesso, il Legislatore, anche in occasione dell'adozione del Codice in materia di protezione dei dati personali (d.lg. n. 196/2003, con cui, peraltro, è stata recepita anche la direttiva 2002/58/CE)[2], ha ribadito (art. 140) le scelte già effettuate all'epoca dell'emanazione della legge n. 675/1996 e del d. lg. n. 467/2001, ritenendo indispensabile

[2] E' opportuno rammentare che l'attuazione della direttiva ha reso necessaria una proroga del termine originariamente fissato dal Parlamento e dal Consiglio europeo per l'adozione del Codice per la protezione dei dati personali (cfr. art. 1 L. 24 marzo 2001, n. 127; art. 26 L. 3 febbraio 2003, n. 14). Sul punto, vedi G. BUSIA, "*Proroga di sei mesi per il Testo Unico privacy*", in Guida al diritto, 2003, n. 8, pag. 79 e ss.. L'Autore ha altresì evidenziato come in sede comunitaria, una volta constatata una crescente convergenza fra i settori delle telecomunicazioni, dei media e delle tecnologie dell'informazione, si sia scelto di "*assoggettare tutte le reti di trasmissione e i servizi correlati a un unico quadro normativo*" che, anziché conformare le regole ad una specifica tecnologia, è basato su un approccio indifferente ("neutro") ai possibili modelli tecnologici utilizzabili. In precedenza, il principale esempio di regolamentazione tecnologicamente neutrale era costituito dal *Model Law on Electronic Commerce*, approvato dall'UNCITRAL *(United Nation Commission on International Trade Law*) nel 1996 ed adottato dall'Assemblea generale delle Nazioni Unite nel dicembre dello stesso anno. Si trattava di uno strumento giuridicamente non vincolante, che si proponeva ai legislatori nazionali dell'epoca quale modello per un tentativo di armonizzazione normativa in tema di commercio elettronico. Sul tema, inoltre, vedi P. PALLARO, "*Libertà della persona e trattamento dei dati personali nell'Unione Europea*", in Contratti comm. internaz., 2002, XVII, p. 181.

stimolare e favorire, attraverso il qualificato intervento del Garante, un'attività di autoregolamentazione di settore per disciplinare compiutamente i trattamenti di dati personali effettuati a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale.

Tale attività, quindi, si concretizzerà nell'adozione di un apposito codice di deontologia e di buona condotta, il cui rispetto, ai sensi dell'art. 12, comma 3 del d. lg. n. 196/2003, costituirà condizione essenziale per la liceità e correttezza del trattamento dei dati personali[3].

3. I programmi di fidelizzazione e la profilazione nell'ambito della grande distribuzione.

Nel corso del tempo, il Garante ha ricevuto vari reclami e segnalazioni sui trattamenti di dati effettuati in occasione dell'impiego di carte o tessere di "fidelizzazione" volte a creare, mediante il riconoscimento di alcuni vantaggi, un rapporto duraturo con la clientela per acquisti e servizi.

L'Autorità ha quindi colto l'occasione per fissare, attraverso l'adozione di uno specifico **provvedimento generale del 24 febbraio 2005**, delle prescrizioni che riguardano in via generale tutti i tipi di "carte" nel settore della c.d. grande distribuzione (doc. web n. 1103045).

In proposito, sul piano sistematico, è stato rilevato che il rilascio di tali carte –cui si accompagna, solitamente, la compilazione di un modulo di adesione o di un questionario- e la loro utilizzazione –che determina la

[3] In proposito, con specifico riferimento al decreto legislativo n. 467/2001, che già conteneva un'identica previsione, vedi F. CASAROSA, *Innovazione e continuità nei codici deontologici e/o di buona condotta ex art. 20 del d. lgs. 467/01: il caso del marketing diretto*, in *Dir. Inform.*, 2002, nn. 4/5, pag. 849 e ss..

registrazione di acquisti di beni e servizi- comportano un trattamento di dati personali dei clienti e, a volte, dei loro familiari.
Spesso e volentieri, però, accanto ai dati anagrafici ed ai recapiti (anche di posta elettronica), sulla scorta di informative assai generiche, che non indicano con precisione neanche tutte le finalità cui il trattamento dei dati è preordinato, vengono raccolte anche altre informazioni, che si rivelano non necessarie per attribuire i vantaggi collegati alla carta: basti pensare al titolo di studio, alla professione, agli interessi, alle abitudini, alle preferenze, alle modalità di acquisti, ecc..
In tali casi, consumatori e relativi nuclei familiari, nel ricevere i vantaggi legati alla fidelizzazione, sono monitorati in dettaglio nei loro comportamenti, vengono profilati anche all'interno di specifiche banche dati e fatti oggetto di raffronto con altri clienti, senza esserne del tutto consapevoli; inoltre, possono essere definiti anche profili individuali o di gruppo (c.d. *cluster*, ovvero segmenti di clientela con caratteristiche omogenee) e propensioni al consumo, senza che i singoli interessati abbiano potuto prestare un effettivo consenso al riguardo.
E ciò a tacere dell'instaurazione di eventuali contatti diretti con la clientela per operazioni di *marketing*, comunicazioni commerciali o pubblicitarie, vendite dirette o ricerche di mercato, effettuati da chi rilascia le carte o da terzi.

Ciò premesso, **le principali prescrizioni fissate dal Garante in relazione alle principali finalità per le quali i dati personali degli interessati sono di regola raccolti e trattati –**e cioè la fidelizzazione in senso stretto, la profilazione mediante analisi di abitudini e scelte di consumo e il marketing diretto- possono essere così riassunte:

1) Necessità dell'osservanza dei fondamentali principi posti dagli artt. 3 ed 11 del Codice privacy (necessità, liceità, correttezza, qualità dei dati e proporzionalità).
2) Per quanto concerne il principio di necessità, i sistemi informativi e i programmi informatici devono essere configurati, già in origine, in modo da ridurre al minimo l'utilizzo di informazioni relative a clienti identificabili, sicché il trattamento dei dati personali dei clienti deve reputarsi illecito laddove le relative finalità –ed in particolare la profilazione- risultino perseguibili attraverso l'impiego di dati anonimi o solo indirettamente identificativi;
3) In relazione al principio di proporzionalità, tutti i dati personali trattati e le relative modalità di trattamento debbono essere pertinenti e non eccedenti rispetto alle finalità perseguite.
4) L'eventuale utilizzazione di dati sensibili, di regola non è ammessa per nessuna delle finalità di cui sopra, salvo il caso in cui il loro trattamento sia effettivamente indispensabile in relazione allo specifico bene o servizio richiesto e sia stato autorizzato dal Garante, oltre che acconsentito per iscritto dall'interessato. Ciò vale anche per eventuali ricerche di mercato, sondaggi ed altre ricerche campionarie (aut. gen. n. 5/2008).

Con specifico riferimento, poi, alla **c.d. "fidelizzazione" in senso stretto**, il Garante ha precisato che possono essere trattati solo i dati necessari per attribuire i vantaggi connessi all'utilizzo della carta.
In particolare, si tratta:

- dei dati direttamente correlati all'identificazione dell'intestatario della carta, e quindi "in primis" delle informazioni anagrafiche;

- dei dati eventualmente relativi al volume di spesa globale progressivamente realizzato (e cioè senza i riferimenti di dettaglio ai singoli prodotti), nella misura in cui sia realmente necessario trattarli –e soprattutto conservarli- per attribuire i vantaggi e per il solo tempo a ciò strettamente necessario. L'eventuale conservazione di dati di dettaglio relativi a particolari tipologie di beni o servizi acquistati, o ai vantaggi conseguiti (punti, premi, bonus) non è di regola necessaria, specie ove si persegua la sola finalità di fidelizzazione; nei casi particolari in cui essa sia lecita, deve essere rispettato il principio di proporzionalità.

Ove venga perseguito lo scopo della **"profilazione" della clientela**, è stato evidenziato che la relativa attività, che può riguardare sia i singoli individui, sia eventuali gruppi, spesso e volentieri può essere svolta impiegando solo dati anonimi o non identificativi (ex.: un codice numerico), senza che risulti necessaria una relazione tra i dati che permettono di individuare i singoli interessati e le indicazioni analitiche relative alla loro sfera personale (gusti, preferenze, abitudini, bisogni e scelte di consumo). In tali ipotesi è obbligatorio non utilizzare dati identificativi.

Negli altri casi, le informazioni che si intende acquisire (sia all'atto dell'adesione del cliente all'iniziativa, sia in caso di registrazione dei singoli beni e servizi) e le rispettive modalità di trattamento debbono essere pertinenti e non eccedenti rispetto alla tipologia dei beni commercializzati e dei servizi resi.

Il rispetto dei principi di pertinenza e di non eccedenza, poi, è necessario anche ove di intenda registrare le informazioni in banche

dati, le quali, oltre tutto, non debbono risultare interconnesse (o fonte di intrecci e raffronti di dati) con quelle utilizzate per la fidelizzazione in senso stretto.

Per quanto concerne, invece, **la finalità di "marketing" diretto**, possono essere raccolti ed utilizzati i dati pertinenti e non eccedenti per l'invio di materiale pubblicitario –anche attraverso riviste di settore- o di comunicazioni commerciali o per la vendita diretta. Si tratta, di regola, dei soli dati direttamente correlati all'identificazione dell'intestatario della carta o di suoi familiari, ovvero di persone indicate da costui. L'eventuale utilizzazione di dati personali derivanti dalla profilazione dev'essere oggetto di un consenso differenziato dei diretti interessati.

Tutto ciò premesso, **le restanti prescrizioni hanno avuto ad oggetto i fondamentali profili dell'informativa, del consenso al trattamento, i tempi di "data retention", gli obblighi di notificazione presso il registro generale dei trattamenti e di adozione delle misure di sicurezza**.

In ordine all'informativa, essa dev'essere fornita al cliente in modo chiaro e completo, anche con formule sintetiche e colloquiali, prima del conferimento dei dati e del rilascio della carta, proprio allo scopo di consentire non solo un'adesione pienamente consapevole alle proposte, ma ancor prima un consenso ai dati da fornire, specie riguardo alla profilazione o al *marketing*.
Ove inserita all'interno di moduli, essa dev'essere adeguatamente evidenziata e collocata in modo autonomo e unitario in un apposito

riquadro, così da essere agevolmente individuabile rispetto ad altre clausole regolamentari eventualmente riportate; inoltre, specifica evidenza dev'essere riservata alle caratteristiche dell'eventuale attività di profilazione e/o di *marketing*, nonché all'intenzione di cedere a terzi ben individuati i dati per specifiche finalità.

Circa il consenso, esso non risulta necessario qualora il trattamento sia preordinato alla **fidelizzazione in senso stretto**, trattandosi di eseguire obblighi derivanti da un contratto del quale è parte lo stesso interessato **(art. 24, comma 1, lett. b) del Codice).**

Invece, in relazione ad ogni altra finalità del trattamento che possa comportare l'identificabilità dell'interessato -in particolare la profilazione, le ricerche di mercato ed il marketing- è necessaria la previa acquisizione di un consenso specifico, informato e distinto, il quale dev'essere quantomeno documentato per iscritto dal titolare del trattamento, salvo il caso in cui debbano essere trattati dati sensibili, allorché è necessario che sia reso per iscritto direttamente dall'interessato.

Relativamente ai tempi di conservazione dei dati, invece, il principio di base da osservare è quello secondo cui i dati personali dei quali non è necessaria la conservazione in relazione agli scopi per i quali sono stati trattati debbono essere cancellati o trasformati in forma anonima.

In ogni caso, i dati relativi al dettaglio degli acquisti con riferimento a clienti individuabili possono essere conservati per finalità di profilazione o di marketing per un periodo di tempo non superiore, rispettivamente, a 12 e 24 mesi dalla loro registrazione, salva la reale

trasformazione in forma anonima che non permetta, anche indirettamente o collegando altre banche di dati, di identificare gli interessati.
Eventuali intenzioni di trattare i dati oltre tali termini potranno essere attuate solo previa valutazione (ed autorizzazione) del Garante, così come previsto dall'art. 17 del Codice (c.d. *prior cheking*).

Per quanto concerne la notificazione, essa, ai sensi dell'art. 37, comma 1, lett. d) del Codice è obbligatoria (tra l'altro) per i trattamenti di dati effettuati con l'ausilio di strumenti elettronici volti a definire profili di consumatori o ad analizzarne abitudini e scelte in ordine ai prodotti acquistati.

Tutto ciò premesso, il Garante ha ritenuto che i dati eventualmente trattati a fini di profilazione o di ricerche di mercato siano conservati con adeguate modalità che portino a limitare l'ambito di circolazione dei dati allo stretto indispensabile, circoscrivendo qualitativamente e quantitativamente il numero di addetti aventi eventuale accesso alle informazioni; inoltre, dev'essere escluso l'uso di sistemi e programmi che permettano, fuori dei casi consentiti, una ricostruzione organica di scelte, comportamenti e profili di interessati identificabili non soggetta alle previe valutazioni del Garante ai sensi del richiamato art. 17 del Codice.

I principi generali fissati nel provvedimento del Garante del 24 febbraio 2005 sono stati riaffermati in successive occasioni, nella quali il Garante si è nuovamente trovato ad affrontare la problematica della profilazione e della fidelizzazione nella grande distribuzione.

Degno di nota è il caso in cui il Garante, a seguito di specifici accertamenti, ha vietato ad una famosa società commerciale il trattamento dei dati personali raccolti per il rilascio alla clientela di "carte di fedeltà" ed utilizzati anche a fini di *marketing* in modo illecito, prescrivendo, al contempo, specifiche misure per conformare a legge i futuri trattamenti di dati (**provvedimento 24 maggio 2006**, doc. web n. 1298784).

In particolare, il Garante aveva constatato che l'informativa fornita ai clienti non era chiara e non consentiva loro di comprendere quali effetti comportasse il trattamento dei dati. In particolare, la società non aveva indicato, tra le finalità perseguite, né l'attività di profilazione nè la successiva comunicazione dei dati dei clienti ad una banca (operante in *partnership*) per l'eventuale sollecitazione ad avvalersi di un fido: infine, veniva condizionato il rilascio della carta al consenso del cliente all'uso dei dati anche per finalità di *marketing* e di profilazione, non permettendo così agli interessati una scelta effettivamente libera.

Il Garante, dichiarando sotto diversi profili illecito il trattamento dei dati effettuato dalla società e vietando l'ulteriore utilizzazione dei dati raccolti, ha prescritto l'adozione di misure per rendere i futuri trattamenti di dati personali conformi alle norme del Codice, stabilendo, in particolare, che l'informativa resa agli interessati fosse riformulata, in modo tale da indicare con maggiore chiarezza gli usi fatti riguardo ai dati personali dei clienti e i destinatari dei dati stessi. Inoltre, l'Autorità ha altresì affermato che gli interessati debbono poter usufruire dei vantaggi connessi al rilascio delle carte di fidelizzazione, anche se non acconsentono al trattamento dei dati per comunicazioni commerciali o ricerche di mercato: infatti, il consenso al trattamento

dei dati dev'essere autonomo, libero e specifico in riferimento alle distinte finalità per le quali il trattamento stesso avviene.

Ma i fenomeni delle carte, dei programmi di fidelizzazione e della profilazione hanno formato oggetto di accertamento anche nell'ultimo biennio, coinvolgendo non solo il settore della grande distribuzione, ma anche quello della telefonia, dei trasporti e dei viaggi.

Con specifico riguardo al settore telefonico, all'esito di una complessa attività istruttoria volta a verificare lo stato dell'attività di "profilazione" effettuata da alcuni "fornitori" (nel caso specifico, gestori telefonici) che mettono a disposizione del pubblico servizi di comunicazione elettronica su reti pubbliche di comunicazione,[4] è emerso che in alcuni casi i dati personali dei rispettivi clienti[5] vengono aggregati in categorie omogenee (cd. *cluster*), secondo parametri predefiniti che ciascun titolare individua di volta in volta a seconda delle specifiche esigenze aziendali (cd. analisi di *business intelligence*).

E' evidente che la disponibilità in capo ai fornitori di tali tipologie di dati ha un enorme valore informativo, in quanto, attraverso il confronto e l'utilizzo delle informazioni attinenti alla clientela, è possibile monitorare l'andamento economico della società e, eventualmente, progettare specifiche campagne di *marketing*.

[4] Consistenti, esclusivamente o prevalentemente, «*nella trasmissione di segnali su reti di comunicazioni elettroniche*» (art. 4, comma 2, lett. d) ed e), del Codice).

[5] I dati, in linea di massima, sono quelli di natura contrattuale e quelli relativi ai consumi effettuati, dai quali è possibile inferire informazioni ulteriori sui singoli interessati, quali la fascia di consumo, il livello di spesa sostenuto ad intervalli regolari, i servizi attivi su ciascuna utenza.

Alla luce di questa realtà, che implica profili di tutela della riservatezza degli utenti, il Garante in data **25 giugno 2009** ha ritenuto di emanare un apposito **provvedimento di carattere generale**[6], con il quale, ai sensi degli artt. 143, coma 1, lett. b) e 154, comma 1, lett. c) del d. lgs. n. 196/2003, ha prescritto ai suddetti fornitori specifiche regole in materia di profilazione della clientela.

Dall'ambito oggettivo del provvedimento, ovviamente, esulano i dati c.d. anonimi, mentre le disposizioni in esso contenute si applicano sia alle ipotesi in cui l'attività di profilazione abbia ad oggetto dati personali individuali, sia a quelle in cui si tratti di dati personali aggregati (derivanti da dati personali individuali dettagliati[7]).

Inoltre, il provvedimento non tocca né la disciplina di cui all'art. 123 del d. lgs. n. 196/2003 (relativa alla conservazione dei dati per finalità di fatturazione), né quella del successivo art. 132 (concernente la conservazione e sicurezza dei dati di traffico telefonico e telematico, per l'accertamento e repressione dei reati.

Nel provvedimento, sostanzialmente, si afferma che ove l'attività di profilazione abbia ad oggetto dati personali individuali, essa può ritenersi consentita solo se risultino rispettati i principi di necessità (art. 3) e di proporzionalità del trattamento (art. 11), e sempre che il titolare del trattamento (e cioè la società telefonica) sia in grado di documentare per iscritto un consenso informato, libero e specifico, manifestato dall'interessato per tale particolare finalità.

E' inutile dire che tale consenso, se reso, ricomprende sicuramente anche il trattamento di dati personali aggregati.

---

[6] Doc. web n. 1629107, reperibile sul sito istituzionale *www.garanteprivacy.it*.
[7] Ad esempio, dati anagrafici e di traffico.

Allorché, invece, il fornitore intenda utilizzare per la profilazione dati personali aggregati per i quali non risulti acquisito il consenso degli interessati, allora egli è tenuto ad esperire la particolare procedura di cui all'art. 17 del d.lgs. n. 196/2003 (c.d. "*prior cheking*"), che il legislatore ha riservato ai trattamenti che presentano rischi specifici.[8]

In questo caso il livello del rischio per l'interessato è direttamente connesso alla maggiore o minore profondità del livello di aggregazione impostato, nonché dalle modalità tecniche con cui viene effettuato il trattamento.

A tal proposito, infatti, lo stesso Garante, nel testo del provvedimento, ha ritenuto di evidenziare immediatamente **i parametri su cui deve basare le proprie valutazioni nell'ambito della specifica procedura ex art. 17**.

Essi sono i seguenti:

- i dati personali oggetto dell'attività di profilazione, ancorché derivino da dati originari dettagliati di cui il titolare continua a disporre per finalità gestionali ed esigenze operative previste anche per legge, devono essere esclusivamente dati aggregati dai quali, nell'ambito dei sistemi dedicati alla profilazione, non sia possibile risalire a informazioni dettagliate relative a singoli interessati;

- i dati personali aggregati oggetto di profilazione devono essere contenuti in uno o più sistemi appositamente dedicati alla profilazione, funzionalmente separati dai sistemi

[8] Il caso più frequente si verifica per l'installazione sui posti di lavoro dei sistemi di rilevazione biometrica, spesso e volentieri associati anche a tecniche di videosorveglianza.

originari che costituiscono la fonte del dato aggregato e da ulteriori eventuali sistemi utilizzati dal titolare per altre finalità (ad esempio *marketing*);

- i dati personali aggregati oggetto dell'attività di profilazione, sia quando si riferiscano ad un interessato, sia quando si riferiscano ad una pluralità di interessati, devono essere sottoposti ad un processo in grado di impedire l'immediata identificabilità dei singoli interessati;

- gli incaricati che svolgono l'attività di profilazione devono disporre di un profilo di autenticazione limitato e diverso da quello di coloro che svolgono eventuali ulteriori attività, anche successive alla profilazione;

- i dati personali oggetto dell'attività di profilazione devono essere conservati per periodi di tempo limitati, decorsi i quali devono essere cancellati.

Infine si rammenta che il trattamento per finalità di profilazione, qualunque sia il tipo di dati impiegati (cioè "individuali" o "aggregati"), ai sensi dell'art. 37, comma 1, lett. d) del d. lgs. n. 196/2003 è soggetto all'obbligo di notificazione.

4. La tecnologia Rfid: le c.d. "etichette intelligenti".

Il Garante si è trovato anche nella necessità di fissare precise garanzie e prescrizioni per coloro che intendono produrre ed utilizzare le c.d. "etichette intelligenti", ossia quei minuscoli *chip* a radiofrequenza (detti anche sistemi *Rfid*, *Radio Frequency Identification*) attivati da lettori ottici, che oramai trovano larga applicazione nell'ambito delle aziende, degli esercizi commerciali, della grande distribuzione, allo scopo di

ottenere una serie di vantaggi, anche per il consumatore, quali la migliore gestione dei prodotti aziendali, la maggiore rapidità delle operazioni commerciali, l'agevole rintracciabilità dell'origine di particolari prodotti, il controllo degli accessi a luoghi riservati.

Tali sistemi possono essere usati anche da soggetti pubblici o privati per scopi ulteriori, quali l'identificazione personale o la tutela della salute; in proposito, molte discussioni stanno nascendo in ordine all'eventualità – già realizzata – di impiantare *microchip* sottopelle, tanto che alcune autorità garanti in Europa hanno già considerato tali utilizzazioni scarsamente compatibili sul piano della protezione dei dati personali.

Per quanto concerne, però, il settore maggiormente interessato all'applicazione di tali tecnologie, ossia quello del *marketing*, si è appurato che alcune forme di utilizzazione, che non si limitano a tracciare il prodotto per garantire l'efficienza del processo di produzione industriale, possono determinare vere e proprie forme di controllo sulle persone, come tali contrarie alla normativa sulla *privacy*: infatti, in tal modo, si possono potenzialmente raccogliere numerose informazioni sulle abitudini dei consumatori a scopo di profilazione, e si possono addirittura tracciare i percorsi effettuati dagli stessi, controllandone la posizione geografica o verificando la tipologia di prodotti usati, indossati o trasportati.

Inoltre, ulteriori problematiche possono insorgere dall'adozione di *standard* comuni, idonei a favorire da parte di terzi la "lettura" o un "intervento" sui contenuti delle etichette (ex.: mediante la loro riscrittura); tali rischi possono aumentare nel caso in cui le tecnologie *Rfid* si integrino con infrastrutture di rete, come telefonia ed Internet, nonché in ragione dello stesso futuro sviluppo tecnologico, che

potrebbe giungere a consentire una "lettura" delle etichette a distanze sempre maggiori.

Ciò premesso, il Garante, **con il provvedimento generale del 9 marzo 2005** (doc. web n. 1109493), è intervenuto in materia, fissando i seguenti punti fondamentali:

1) le persone debbono essere sempre adeguatamente informate sull'utilizzazione dei sistemi *Rfid* e dell'esistenza dei lettori ottici che attivano le etichette; sotto tale profilo, la presenza di avvisi nei luoghi in cui tali tecniche sono impiegate non esime dall'apporre una specifica informativa sugli stessi oggetti e sui prodotti che recano siffatte etichette;
2) l'utilizzazione di tali sistemi *Rfid*, ove determini il trattamento di dati personali, è ammessa solo con il consenso espresso e specifico dell'interessato, ottenuto senza alcuna pressione o condizionamento di costui (ciò, ovviamente, a meno che non ricorra nel caso specifico uno dei presupposti di legge equipollenti al consenso);
3) deve essere sempre garantita agli interessati la possibilità di asportare, disattivare o interrompere gratuitamente e in maniera agevole il funzionamento delle *Rfid* al momento dell'acquisto del prodotto su cui è apposta l'etichetta;
4) allorché la tecnologia in questione venga impiegata per la verifica degli accessi a determinati luoghi di lavoro (riservati), debbono essere previste adeguate cautele per i diritti e le libertà dei lavoratori, soprattutto allo scopo di non consentire ipotesi di controllo a distanza dei medesimi.
5) I *microchip* sottopelle possono essere ammessi solo in casi eccezionali, per comprovate e giustificate esigenze di tutela della

salute delle persone, e debbono permettere comunque la loro rimozione e l'interruzione del relativo trattamento di dati su richiesta dell'interessato. Inoltre, i soggetti che intendono utilizzare tali *microchip* debbono sottoporre tali sistemi a verifica preliminare dell'Autorità.

6) Infine, debbono essere sempre rispettati i principi di proporzionalità (in relazione agli scopi che si intendono perseguire), di finalità della raccolta e di conservazione dei dati. Allo stesso modo va rispettato il dovere di adottare adeguate misure di sicurezza in relazione ai dati conservati.