DIGITAL PROFILING & PRIVACY[1]

di

Alessandro di Maggio[2] e Telesio Perfetti[3]

[2] Consulente legale, esperto in privacy, diritto dell'informatica e delle nuove tecnologie. Membro del comitato di Redazione di «ComputerLaw.it» "rivista telematica di informatica giuridica e diritto dell'informatica, in qualità di responsabile per il settore "e-commerce" "e-procurement". Già collaboratore per il master in e-procurement presso l'università di Roma "Tor Vergata", in qualità di tutor, è docente per la «Quality Key», società per la consulenza e la formazione, per i corsi di formazione sulla "tutela della privacy", "l'e-commerce", "i contratti telematici", etc.

[3] Giurista esperto in ICT Law (diritto delle nuove tecnologie), nonché in diritto civile e in diritto penale. È collaboratore dello Studio Legale F&D di Roma e dello Studio Legale Lai di Roma. Collabora attualmente come docente presso il Master universitario di II livello "Diritti della persona e nuove tecnologie" - Università degli Studi di Roma "La Sapienza" (direttore Prof. Stefano Rodotà). È altresì docente in corsi di formazione per aziende e studi professionali in materia di privacy, e-security ed e-commerce. È tra l'altro autore di pubblicazioni in materia di diritto dell'informatica ed informatica giuridica e membro del comitato di redazione della rivista telematica "ComputerLaw.it – Informatica e Diritto", nella quale si occupa, in qualità di responsabile, delle aree "e-privacy" e "cybercrimes".

1. Introduzione.

Le nuove frontiere dell'economia aziendale si basano, da sempre, nel cercare la giusta combinazione tra l'innovazione tecnologica, l'innovazione organizzativa e l'innovazione dei processi aziendali, in modo da facilitare nuovi modi di produrre e distribuire beni e servizi.

L'espressione di questo connubio si palesa oggi nella crescente mole di investimenti che le aziende realizzano nelle tecnologie dell'informazione e della comunicazione (ICT), ritenute in grado di fornire l'infrastruttura attraverso la quale operare in tempo reale e su scala mondiale.

Si sta passando, quindi, dal considerare "l'informazione" come un bene economico all'informazione come strumento in grado di creare valore economico[4].

Altro rilevante cambiamento si ritrova nell'idea del consumatore non più come membro di un gruppo omogeneo, privo di diversificazioni, ma in quanto individuo. Tendono ad affermarsi, anche a causa dei moderni sistemi di comunicazione interattiva, nuovi metodi di relazione fondati sulla personalizzazione dei messaggi pubblicitari: il consumatore si trova così al centro di una rete di messaggi che tendono ad indurlo all'acquisto facendo leva sui suoi specifici interessi e bisogni. Si è, ormai, realizzato il passaggio dal "mercato rivolto alle masse" al "mercato rivolto agli individui".

L'uso delle nuove tecnologie quale strumento per ampliare la propria quota di mercato spinge le aziende, con sempre maggiore frequenza, - sia che esse operino direttamente su internet, sia che utilizzino la rete come semplice vetrina - ad utilizzare sistemi in grado, da un lato, di individuare e acquisire nuovi clienti, e dall'altro, una volta raggiunto siffatto obbiettivo, a fare in modo che questi rimangano "legati" all'azienda nelle future transazioni.

Si ricorda che i sistemi maggiormente in uso e basati sulle nuove tecnologie per le finalità di cui sopra sono il "*web marketing*"[5] e il "*direct marketing*"[6] con specifico riferimento all'acquisizione della clientela ed il *Customer Relationship Management* (CRM) per la sua *fidelizzazione*.

In quest'ultimo rientrano, oltre all'aspetto gestionale, sia l'individuazione, la segmentazione e l'acquisizione del cliente, che la fidelizzazione e lo sviluppo ulteriore della relazione. Tutto ciò, al di là della tecnologia di CRM utilizzata, permette all'azienda di ottenere dati e informazioni preziose per personalizzare i servizi, per renderli sempre più vicini alle esigenze dei

---

[4] V. E. Hofmann, "*Economia e Innovazione Tecnologica dopo la rivoluzione di Internet*", MediaDuemila, marzo 2002.

[5] Il web marketing è l'attuazione della strategia di marketing dell'azienda che si traduce e si realizza tramite il sito internet è l'insieme delle tecniche e degli strumenti che consentono di sviluppare i rapporti commerciali (acquisti, pubblicità, vendite, assistenza alla clientela, etc.) tramite il Web. Il web marketing è anche ogni azione a pianificazione che abbia come finalità il ROI (return on investment) di un progetto on-line, è ideazione di un progetto, è il coordinamento della sua realizzazione, è l'analisi finale, è la gestione di ciò che ne segue la messa in opera, è la sua promozione e la gestione del feedback. Ogni progetto (con obiettivi) fatto in internet deve essere coordinato da un piano di web marketing. Spesso si confonde il WM con la semplice promozione o pubblicità di un sito in Internet.

[6] Il direct marketing è un sistema pianificato di registrazione, analisi e tracciabilità delle caratteristiche salienti di un customer, atte a sviluppare un'efficiente strategia di relazione.

clienti, per aumentarne il valore e, spesso, per anticiparne i bisogni futuri. In sostanza, il CRM è interamente focalizzato sull'attenzione al cliente.

Nel porre al centro dell'attenzione l'utente si tende ad una visione sempre più integrata e complessiva del rapporto con lo stesso, al fine di una maggiore personalizzazione del servizio. Questo "processo" non riguarda solamente le aziende private, ma di recente anche le pubbliche amministrazioni[7].

Per poter attuare tali sistemi, le aziende devono necessariamente reperire un elevato numero di informazioni idonee a tracciare le abitudini dei clienti: ciò può avvenire anche e soprattutto tramite software dedicati, e prende il nome di **profilazione**.

Una simile esigenza implica che le politiche di CRM debbano far leva su tutta una serie di informazioni che dovranno necessariamente essere approfondite e personali, e che, solo inizialmente, proverranno dall'esterno (database, siti web, etc.), mentre, in seguito, saranno continuamente arricchite mediante l'allestimento di un sistema informatico in azienda.[8]

Se è vero che le aziende sono fortemente orientate all'utilizzo di siffatti sistemi, al contempo (soprattutto quando il cliente è un consumatore[9]) è altrettanto doveroso per le medesime garantire il "giusto" utilizzo dei dati reperiti al fine di non invadere la privacy dei soggetti profilati: esigenza, quest'ultima, che non viene quasi mai presa in considerazione.

Mentre, infatti, in tema di *customer satisfaction* le aziende investono ingenti risorse, non altrettanto può dirsi con riferimento ai sistemi di misurazione della qualità derivante dal corretto trattamento dei dati personali, probabilmente perché non lo si considera di particolare interesse economico.

Al contrario, la questione della tutela della privacy assume una rilevanza fondamentale, sia per lo sviluppo dell'economia dei nuovi mercati, sia dal punto di vista del rispetto della dignità e della riservatezza degli individui: il diritto alla tutela dei dati personali è destinato a svolgere una funzione fondamentale per disegnare i futuri assetti del rapporto tra imprese e consumatori.

Se la sensibilità verso la tutela della riservatezza dei dati personali venisse trascurata, si rischierebbe, infatti, di assistere a due spiacevoli fenomeni: da una parte rinverremo un consumatore assediato, denudato ed influenzabile, conosciuto e scrutato quotidianamente dai "trafugatori di informazioni personali" che, in mancanza di regolamentazioni e controlli, potrebbero usare questi dati per sollecitare acquisti inutili o dannosi e stimolare bisogni non reali né attuali; dall'altra si potrebbe realizzare l'incresciosa prospettiva di un mercato bloccato che, messo nell'impossibilità di dialogare con il consumatore (tradito) e di stabilire un rapporto diretto e fiduciario con il cliente, sarebbe destinato a ritornare sui suoi passi e a riutilizzare quei metodi invadenti e ridondanti della pubblicità di massa, ormai considerati forme di comunicazione obsolete.[10]

---

[7] Sul punto è molto interessante l'innovazione apportata dall'**art. 7** (Qualità dei servizi resi e soddisfazione dell'utenza) del D.Lgs. 82/2005, il c.d. **Codice dell'Amministrazione Digitale:** «Le pubbliche amministrazioni centrali provvedono alla riorganizzazione ed aggiornamento dei servizi resi; a tale fine sviluppano l'uso delle tecnologie dell'informazione e della comunicazione, sulla base di una preventiva analisi delle reali esigenze dei cittadini e delle imprese, anche utilizzando strumenti per la valutazione del grado di soddisfazione degli utenti.»

[8] V. D. Bergantin e R. Galbiati, "Il *rispetto della privacy risorsa chiave del CRM - Conferenza internazionale privacy: da costo a risorsa*", 5-6 dicembre 2002.

[9] La persona fisica che agisce per scopi estranei all'attività imprenditoriale o professionale eventualmente svolta.

[10] Per approfondimenti v. G. Rasi, "*La privacy come qualità nella moderna economia - 26ª Conferenza Internazionale sulla Privacy e sulla Protezione dei Dati Personali*", Wroclaw (PL), 14, 15, 16 settembre 2004.

2. Consumer profiling e privacy: due aspetti fondamentali.

Il problema del rispetto della tutela della privacy dei consumatori deve essere affrontato dalle imprese sotto due differenti punti di vista: da un punto di vista sociale, in riferimento alla capacità della privacy di impattare sulle variabili cognitive del cliente alla base del processo di consolidamento della relazione con l'impresa; da un punto di vista etico, in riferimento alla necessità delle aziende di adottare comportamenti non opportunistici nei confronti dei clienti per non minare la propria capacità relazionale; si può, quindi, parlare di *customer loyalty*, termine che sta ad indicare che il comportamento etico dell'azienda è quello di incrementare la fiducia del cliente.[11]

Dal punto di vista sociale si è cercato di individuare quali siano le cause e le conseguenze relazionali rispetto alla sensibilità che i consumatori avvertono nei confronti della propria privacy.

Alcuni studi hanno individuato una serie di analogie esistenti tra il livello di fiducia verso l'impresa, il livello di privacy e la disponibilità relazionale del consumatore. Più precisamente, si è osservato che, sia il livello di privacy che il consumatore richiede, sia la fiducia verso l'impresa, impattano sulla sua volontà relazionale: una più alta fiducia incide positivamente sulla volontà relazionale del cliente, mentre la privacy impatta su tale volontà in termini negativi; maggiore è la preoccupazione per tale problematica, minore è la possibilità che si instauri una relazione duratura con l'impresa.

In effetti, un'azienda che non manifesti interesse per la privacy dei propri clienti (o comunque dei consumatori in generale) potrebbe minare la percezione del consumatore sulla sua affidabilità e, dunque, influire negativamente sul processo di sviluppo relazionale, facendo apparire logico supporre l'esistenza di una correlazione negativa tra la dimensione motivazionale della fiducia ed i problemi di privacy dei clienti riguardo all'acquisizione e all'uso dei dati personali.

Dal punto di vista etico, uno dei fattori che agisce sul livello di *loyalty* del cliente è la percezione del coinvolgimento dell'organizzazione nella tutela delle sue informazioni. L'adozione di comportamenti etici è in grado di differenziare le aziende che agiscono senza il rispetto per la privacy da quelle che rispettano tale condizione. Parlare di etica "relazionale", quindi, significa impiegare le politiche e le strategie aziendali per ridurre le incertezze dei clienti riguardo al problema della privacy e aumentarne il grado di fiducia e di fedeltà verso l'azienda. I consumatori, infatti, saranno meno preoccupati del potenziale abuso o delle conseguenze negative risultanti dalla raccolta delle loro informazioni se vi è un senso di fiducia verso l'organizzazione.

È stato ampiamente dimostrato che in caso di concorrenza dove i *brand* sono indifferenziati e i prezzi sono uniformati, quindi in situazione di omogeneità dell'offerta, la preoccupazione per la privacy gioca un ruolo rilevante nell'influenzare il comportamento d'acquisto del cliente.

Nonostante ciò, le aziende continuano a focalizzare le risorse esclusivamente sulla acquisizione di dati personali, a volte anche eccessivi rispetto all'effettivo utilizzo e spesso acquisiti

[11] V. D. Bergantin e R. Galbiati, *op. cit.*

con sistemi al limite della legalità (v. paragrafo successivo), piuttosto che tracciare le basi di un rapporto fiduciario basato sulla trasparenza e sulla riservatezza dei dati personali.

3. La "profilazione" del net-consumer

Allo stato attuale nell'ambito dell'*e-commerce* è molto facile schedare o profilare un utente della Rete, considerate le molteplici tracce che egli lascia durante la navigazione (siti visitati, acquisti effettuati, *download*, iscrizioni a servizi di *newsletter* o a *newsgroup* che trattano determinati argomenti, etc.). Grazie alle informazioni che ogni cybernauta lascia sulle autostrade dell'informazione, determinati server creano appositi *database* in cui raccogliere questa immensa mole di dati, utilizzando i quali è possibile tratteggiare un "profilo" potenzialmente completo del navigatore di Internet, per quel che concerne i suoi gusti in materia di consumo, nonché per quel che riguarda altri aspetti più delicati o "sensibili" della propria personalità (scelte e abitudini in materia sessuale, politica, ideologica, religiosa, etc.). In effetti tramite siffatti database vengono elaborati *record*, in cui è possibile ricostruire il tipo di articoli ricercati nonché quelli per i quali sono semplicemente state chieste informazioni o anche il tempo speso per la ricerca. In questo modo la profilazione risulta totale, avendo ad oggetto non solo la merce acquistata, ma altresì quella solo esaminata. Molti siti di e-commerce (es. *Amazon.com*) tengono traccia addirittura degli acquisti per gruppo demografico[12]. Tra l'altro tali database costituiscono una vera e propria fonte di reddito per chi li gestisce, considerando che i dati e le informazioni in essi contenuti sono oggetto di compravendita, con possibilità di ottenere enormi guadagni[13].

In queste situazioni tutelare il proprio "anonimato commerciale" in Rete diventa impresa ardua, se non impossibile da realizzare. Tanto più se si pensa all'uso da parte dei siti web di commercio elettronico dei cd. *"cookies"*, veri e propri marcatori o tracciatori dei percorsi effettuati dal net-user. I *cookies* altro non sono che dati (file di testo) inviati dal server-web al *browser* che li memorizza sul PC per poi restituirli al server ogni qual volta l'utente ritorni a visitare il sito in questione. In tal senso i *cookies* risultano molto utili per la navigazione, la snelliscono e la rendono più veloce. In tali casi si parla anche di *cookies* "buoni" o *"di sessione"*, aiutano la gestione di funzioni come i carrelli elettronici durante gli acquisti *on-line*, hanno una durata limitata e terminano il "tracciato digitale" con la chiusura della connessione dell'utente alla Rete. L'utilità dei *cookies* sta nel fatto che l' *"http"* è un protocollo di comunicazione privo di stato, nel senso che il server non conosce l'utente che visita il sito, cosicché si limita ad inviargli le informazioni di navigazione. Dunque un funzionamento di questo tipo va bene con i siti statici o semplici, mentre la cosa si complica laddove il sito sia dinamico, quindi più complesso, in quanto per es. fornisce prodotti o servizi a pagamento. Si pensi ad una rivista o ad un quotidiano on-line: l'utente, una volta pagato il costo dell'abbonamento, ottiene le credenziali per effettuare il *"login"* (procedura di registrazione e/o autenticazione), che in genere avviene tramite associazione logica *"userid"–"password"*. Ebbene grazie ai *cookies* tali credenziali accompagnano il lettore per tutto il corso della sua visita, senza bisogno che egli si autentichi ogni volta che cambi articolo o passi da una pagina all'altra. Lo stesso può dirsi per la "scheda–acquisti", fornita dal sito a ciascun utente, allo scopo di seguirlo per tutta la durata dell'esplorazione. Ecco perché si dice che i *cookies* consentono di aggiungere informazioni di stato ai protocolli di comunicazione di Internet,

---

12 V. B.Schneier, "Sicurezza Digitale – Miti da sfatare, strategie da adottare", Tecniche nuove, 2001, Cap. 3, p. 28.

13 Stando a quanto riportato nella Newsletter del Garante della Privacy della settimana 11 – 17 Giugno 2001, vi sarebbero state aziende negli USA disposte a pagare circa 500$ per dati e informazioni relativi a ogni nuovo cliente.

quasi si trattasse di un immenso database, i cui dati sono sparsi per milioni di browser presenti in Rete[14]. V'è comunque il rischio che attraverso i *cookies*, il *merchant* riesca a collegare informazioni in precedenza anonime con gli indirizzi dei singoli utenti (in particolare con gli account di posta elettronica). Questa forma di relazione può comportare l'arrivo di messaggi e-mail indesiderati e quindi l'invio di "posta spazzatura" (*spamming*) ovvero i dati degli utenti vengono venduti a terzi. Non solo: taluni *cookies* sono permanenti. In tali casi il titolare del sito Web che li istalla sul PC dell'utente, secondo la normativa italiana, dovrebbe fornire un'idonea e completa informativa (v. art. 13 del D.Lgs. 196/2003, altrimenti noto come *"Codice della Privacy"*), anche in riferimento alla durata, e spiegare altresì il modo per disabilitare questi marcatori. Ma la cosa accade molto di rado. Anzi è proprio l'occultezza dei *cookies* in tali casi a fungere da valido strumento per profilare l'utente/consumatore a sua insaputa, senza tra l'altro che vengano rispettati gli altri obblighi previsti dalla legge (per es. l'obbligo di notificazione).

Da ultimo si ricordi che molte delle banche-dati, che raccolgono notizie sui gusti e sulle abitudini consumeristiche degli utenti della Rete e dei compratori on-line, sono tra loro interconnesse, agevolandosi così lo scambio di preziose informazioni tra aziende operanti nei settori dell'informatica e dell'e-commerce.

La profilazione diventa pertanto per un'azienda efficace strumento per reclamizzare e commercializzare propri prodotti, per inviare pubblicità mirata, per sollecitare e fidelizzare una vasta parte di pubblico e per controllare il mercato attraverso la schedatura delle scelte dei consumatori.

4. La normativa in tema di "profilazione".

Ma cosa prevede la legge italiana in materia di profilazione del consumer tramite l'ausilio di strumenti elettronici? Il riferimento normativo fondamentale è ovviamente contenuto nel Codice della Privacy (di seguito, per brevità, Codice). Tuttavia vi sono numerosi provvedimenti, adottati dal Garante per la protezione dei dati personali (di seguito Garante), che si occupano specificamente dell'argomento. Ci si riferisce in particolare ai provvedimenti sulla *"TV interattiva"* (3/02/2005)[15], sulle *"fidelity cards"* o "carte di fidelizzazione" (24/02/2005)[16], sull'uso delle cd. *"RFID"* o "etichette intelligenti"[17] e sugli adempimenti

---

14 v. ancora B.Schneier, op.cit., cap. 10, p. 135.

15 V. in Bollettino n. 58 del Febbraio 2005, pag. 0 [doc. web n. 1109503]. Cfr. anche il Comunicato stampa del 7/03/2005.

16 V. in Bollettino n. 58 del Febbraio 2005, pag. 0 [doc. web n. 1103045].

17 V. in Bollettino n. 59 del Marzo 2005, pag. 0 [doc. web n. 1109493]. Si ricordi che "RFID" è l'acronimo di "Radio Frequency Identification", tecnica di identificazione di una cosa (es. di un prodotto commerciale) o di una persona tramite radio-frequenze generate da microchip attivati da lettori ottici. Per quel che concerne le etichette intelligenti identificative dei prodotti, esse iniziano a trovare applicazione nell'ambito degli esercizi commerciali e della grande distribuzione allo scopo di ottenere una serie di vantaggi, anche per il consumatore (migliore gestione dei prodotti aziendali, maggiore rapidità delle operazioni commerciali, agevole rintracciabilità dell'origine di particolari prodotti). Tuttavia, precisa il Garante, «alcuni impieghi di questa tecnologia - che non si limitino a tracciare il prodotto per garantire l'efficienza del processo di produzione industriale - possono costituire una violazione del diritto alla protezione dei dati personali e determinare forme di controllo sulle persone: con l'uso di Rfid si potrebbero, infatti, raccogliere innumerevoli dati sulle abitudini dei consumatori a fini di profilazione o essere in grado di tracciare i percorsi effettuati dagli stessi, controllarne la posizione geografica o verificare quali prodotti usa, indossa, trasporta» (cfr. Comunicato stampa del 25 marzo 2005). Nel provvedimento de quo, per il caso di tecniche di RFID associate all'utilizzo di carte di fidelizzazione della clientela e al trattamento di dati relativi a clienti a fini di profilazione commerciale, viene espressamente prescritto il rispetto dei principi di protezione dei dati esplicitati dal Garante nel provvedimento del 24 febbraio 2005 sulle fidelity cards, con specifico riferimento a informativa, consenso, necessità e proporzionalità.

privacy da adottarsi da parte di *"aziende alberghiere"* (9/03/2006)[18]. I principi affermati sono applicabili in via di interpretazione sistematica e analogica anche alle aziende di e-commerce. Si tenterà ora di individuare le direttrici principali da seguire.

1. L'attività di profilazione deve avvenire nel rispetto dei diritti e delle libertà fondamentali della persona umana (art. 2 Codice), con particolare attenzione alla dignità, all'identità, alla riservatezza e al diritto alla protezione dei dati personali. In tal senso vale il divieto di schedare il consumatore a scopi di discriminazione.

2. Deve essere rispettato il "principio di necessità" (art. 3 del Codice), in base al quale i sistemi informatici e i software devono essere configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali e di dati identificativi e da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto la finalità di profilazione deve essere perseguita dai titolari, se e finché è possibile, tramite l'uso di dati anonimi o comunque non identificativi[19] e devono essere evitate tutte quelle informazioni che non sono strettamente necessarie[20].

3. Il trattamento dei dati deve avvenire in modo lecito e corretto (art. 11, comma 1, lett. a) del Codice). Con riferimento specifico alla TV interattiva e alle abitudini davanti al video «non è lecito trattare dati personali relativi a tempi di connessione, visioni di programmi ed eventi, fasce orarie di utilizzazione del mezzo televisivo, interruzioni di ascolto, cambi di canale ed analisi del comportamento in presenza di spazi pubblicitari»[21].

4. Deve essere rispettato il principio di "proporzionalità" del trattamento, sotto il profilo della pertinenza e della non eccedenza dello stesso. In relazione a ciò il Garante, col provvedimento sulle fidelity cards, ha stabilito che:

a) non è lecito utilizzare a fine di profilazione dati *"supersensibili"*, e cioè idonei a rivelare lo stato di salute e la vita sessuale[22];

b) quanto ai tempi di conservazione, vale il principio generale ex art. 11, comma 1, lett. e) del Codice, ai sensi del quale i dati personali dei quali non è necessaria la conservazione in relazione agli scopi per i quali sono stati trattati devono essere cancellati o trasforma-

---

18 V. in Bollettino n. 70 del Marzo 2006, pag. 0 [doc. web n. 1252220].

19 Nel provvedimento sulla TV interattiva è espressamente stabilito che in caso di televoto «deve essere deve essere evitata, fin dal momento della ricezione delle informazioni trasmesse dall'utente, la raccolta e/o la registrazione di dati associabili a persone identificabili, anche quando le domande riguardino solo gradimenti, gusti o preferenze e non siano richieste anche opinioni di natura sensibile su persone, fenomeni sociali o profili politico-religiosi o sindacali. Ricerche di mercato, altre ricerche campionarie e sondaggi devono essere effettuati in forma anonima, evitando l'afflusso di risposte relative a soggetti identificabili, oppure (se ciò è tecnicamente inevitabile) rendendo tali risposte realmente anonime subito dopo la loro raccolta, escludendo a maggior ragione ogni eventuale comunicazione a terzi o diffusione dei dati personali».

20 Ad es., in caso di TV interattiva, nella fatturazione il titolo del film acquistato non deve comparire (cfr. Comunicato stampa del 7/03/2005 cit.).

21 Cfr. Comunicato stampa del 7/03/2005 cit.

22 Cfr. anche Autorizzazione generale del Garante n. 5/2005 al trattamento di dati sensibili da parte di diverse categorie di titolari (http://www.garanteprivacy.it/garante/doc.jsp?ID=1203938).
Con riferimento alla TV interattiva, il Garante ha stabilito che «nel caso in cui, per le specifiche informazioni trasmesse dagli utenti o per le modalità della loro utilizzazione si intenda raccogliere dati sensibili (art. 4, comma 1, lett. d), del Codice), deve tenersi presente che il loro trattamento non è di regola ammesso né per l'ordinaria prestazione di servizi televisivi, né per eventuali finalità di profilazione o fidelizzazione della clientela, fatta salva l'ipotesi eccezionale nella quale il medesimo trattamento sia realmente indispensabile in rapporto ad uno specifico bene o servizio richiesto e sia altresì autorizzato dal Garante, oltre che acconsentito dall'interessato in forma scritta o telematica equiparabile allo scritto. Ciò, vale anche per eventuali ricerche di mercato, sondaggi ed altre ricerche campionarie».

ti in forma anonima; tuttavia i dati relativi al dettaglio degli acquisti con riferimento a clienti individuabili e necessari per scopi di profilazione possono essere mantenuti per un periodo massimo di dodici mesi, salva la reale trasformazione in forma anonima che non permetta, anche indirettamente o collegando altre banche di dati, di identificare gli interessati[23];

c) i database usati per la profilazione non possono (né devono) essere interconnessi, tanto meno possono costituire strumento di intreccio e raffronto di dati con quelli utilizzati per altre finalità, per es. per scopi di fidelizzazione in senso stretto.

5. Il trattamento dei dati personali a scopo di profilazione può essere lecito e corretto solo se trasparente. Pertanto va fornita, ai sensi dell'art. 13 del Codice, un'informativa preventiva (prima cioè che il trattamento abbia inizio)[24], adeguata, chiara e completa di tutti gli elementi richiesti dalla suddetta disposizione. In particolare la finalità di profilazione deve essere indicata puntualmente e con evidenza (in apposita casella separata rispetto ad altre finalità), in modo che il *consumer* ne abbia piena contezza e possa decidere liberamente se prestare o meno il consenso. Allo stesso modo deve essere specificamente individuata anche l'eventuale intenzione da parte del titolare di cedere dati a terzi, soprattutto in riferimento all'ipotesi di vendita di database. L'interessato deve essere reso edotto anche dei diritti che gli spettano ex art. 7, con particolare riferimento:

a) al diritto di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati (comma 3, lett. b);

b) al diritto di opporsi, in tutto o in parte, per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta (comma 4, lett. a).

Ad ogni modo, si possono utilizzare formule sintetiche e colloquiali, purché chiare e non equivoche, evitando rinvii generici a regolamenti di servizio non acclusi per le parti di riferimento. L'informativa inserita all'interno di moduli deve essere adeguatamente evidenziata e collocata in modo autonomo e unitario in un apposito riquadro e risultare altresì agevolmente individuabile rispetto ad altre clausole del regolamento di servizio eventualmente riportato in calce o a margine.

Con specifico riferimento ai *cookies* cd. buoni o legittimi (come quelli di sessione), il considerando 25 della direttiva 2002/58/CE (cd. "Direttiva relativa alla vita privata e alle comunicazioni elettroniche") stabilisce che essi possono essere sì utilizzati come marcatori, purché siano fornite agli utenti informazioni chiare e precise sugli scopi che essi perseguono. Sempre in base al suddetto considerando, gli utenti dovrebbero inoltre avere la possibilità di rifiutare che un *cookie* venga istallato sul proprio terminale e anche di ciò dovrebbe essere fornita un'informazione chiara e precisa.

Ai sensi dell'art. 17 del Codice, il trattamento di dati personali, diversi da quelli sensibili e giudiziari, che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato (come nel caso di monitoraggio e profilazione), resta soggetto e condizionato all'adempimento di specifici obblighi e prescrizioni dettati dal Garante a se-

---

23 Eventuali intenzioni di trattare i dati oltre tali termini potranno essere attuate solo previa valutazione del Garante ai sensi dell'art. 17 del Codice. In caso di cessazione del rapporto deve cessare ogni loro utilizzazione per finalità di profilazione (v. anche art. 16, comma 1, lett. a) del Codice).

24 Per quel che concerne la TV interattiva, il Garante ha stabilito che l'informativa venga fornita sia all'atto della costituzione del rapporto, sia prima di evadere le singole richieste di servizio o sollecitare le risposte degli utenti.

guito di "verifica preliminare" (cd. *"prior checking"*), e cioè antecedente all'inizio del trattamento.

Ovviamente, anche in stretto collegamento con quanto disposto dall'art. 13, è necessario raccogliere l'espresso consenso dell'interessato, ai sensi dell'art. 23 del Codice. Solo se l'informativa è specifica, chiara, completa, allora potrà esservi un consenso libero, informato, consapevole, fermo, serio, ribadito e specifico[25]. Non è corretto che il titolare solleciti il consenso al trattamento in termini generali, es. ricorrendo a formule del tipo: "il consenso è necessario per eseguire obblighi derivanti dalla legge, dal contratto o per finalità commerciali". Dunque non è lecito raccogliere il consenso, ricorrendo ad un'unica nonché generica dichiarazione (quasi si trattasse di una mera clausola di stile), che prescinda dalle finalità perseguite. Nel *form* vanno nettamente distinti i casi in cui il consenso non è necessario (es. per adempiere a obblighi di legge o contrattuali) da quelli in cui è solo facoltativo. Il consenso in definitiva non può essere una condizione per stipulare un qualsivoglia contratto o per ottenere un certo servizio. *Ergo* ancora, se vi sono scopi particolari e non necessari del trattamento (e il caso di profilazione senza dubbio vi rientra) rispetto all'adempimento degli obblighi derivanti dalla legge o dal rapporto contrattuale, essi vanno indicati a parte, in modo da essere suscettibili di un consenso distinto e meramente facoltativo. Resta sempre salva l'applicazione delle ulteriori garanzie ex art. 26 in caso di eventuale trattamento di dati sensibili (consenso scritto[26] *ad substantiam* e autorizzazione del Garante), peraltro (è bene ribadirlo) da evitare in linea di principio per le finalità di profilazione.

Per il caso di trattamento di dati personali a scopo di profilazione tramite l'ausilio di strumenti elettronici, deve essere adempiuto preventivamente ed una sola volta (a prescindere dal numero delle operazioni e della durata del trattamento da effettuare) l'obbligo di notificazione al Garante ex art. 37, comma 1, lett. d) del Codice. Siffatto obbligo risponde a esigenze di trasparenza e va posto in essere con modalità e forme previste dall'art. 38[27].

Al di là delle sanzioni amministrative previste per le ipotesi di omessa e inidonea informativa ovvero omessa notificazione, restano salve le eventuali responsabilità civili per danni (patrimoniali e morali) ai sensi dell'art. 15 del Codice, nonché quelle penali, di cui agli artt. 167 (trattamento illecito di dati personali[28]), 168 (falsità nella notificazione), 169 (omessa

---

25 Nel caso di TV interattiva, se non vi è un distinto e specifico consenso alla profilazione, i dati personali desumibili dal voto televisivo, da sondaggi, acquisti, ecc. non possono essere registrati ed utilizzati per l'una o l'altra di queste finalità. Il consenso al trattamento dei dati neutri o comuni, in tali casi, può essere espresso anche tramite telecomando.

26 La comunicazione in modalità interattiva di dati sensibili da parte dell'utente al fornitore deve essere possibile solo mediante credenziali di autenticazione associate ad una parola chiave riservata, cioè ad una password, che sostituirebbe la firma scritta apposta su modulo cartaceo, in quanto "firma elettronica" semplice o debole. A tal proposito v. l'art. 1, lett. q) del D.Lgs. 82/2005 (cd. Codice delle Amministrazioni digitali), che definisce la firma elettronica come "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica".

27 Ai sensi del comma 2 dell'art. 38, la notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione. Tuttavia, ai sensi del comma 5, il Garante può individuare altro idoneo sistema per la notificazione in riferimento a nuove soluzioni tecnologiche previste dalla normativa vigente.

28 Si pensi ai casi di utilizzo illecito di cookies o banner: potrebbe ravvisarsi il delitto di trattamento illecito di dati personali per difetto del consenso dell'interessato per i fini di profilazione e di cessione di dati a terzi in virtù del combinato disposto degli artt. 167 e 23 del Codice, con eventuale aggravante nei casi di cui all'art. 26. Non v'è dubbio alcuno sul dolo specifico (scopo di profitto) e sulla sussistenza della "condizione obbiettiva di punibilità" (nella specie, il "nocumento", da intendersi quale apprezzabile vulnus o lesione al proprio patrimonio ovvero alla propria riservatezza e libertà di autodeterminazione informatica e informativa, quale diritto al controllo sui propri dati). Ovviamente, considerando la clausola di riserva, potrà ravvisarsi il delitto de quo, sempre che il fatto non costituisca più grave reato, come nel caso di utilizzo di spyware. Si pensi, a tal propo-

adozione di misure di sicurezza) e 170 (inottemperanza ai provvedimenti del Garante[29]) del Codice. Inoltre la condanna per uno dei suddetti reati comporta, quale pena accessoria, la pubblicazione della sentenza (v. art. 172 del Codice).

5. Ambito di applicazione delle norme.

Secondo quanto disposto dall'art. 5 del Codice (D.Lgs. 196/2003), le norme appena descritte si applicano al «trattamento di dati personali, **anche detenuti all'estero**, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato».

Stabilisce, ancora, lo stesso codice che le norme si applicano «anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea».

Quindi, in base all'appena citato art. 5 del Codice, sono soggetti a rispettare le norme applicabili in caso di profilazione tutte le aziende appartenenti all'unione europea o comunque, anche se extracomunitarie, che utilizzino strumenti situati nel territorio italiano o soggetto alla sua sovranità.

Poniamo, invece, il caso di una società non appartenente all'Unione europea, che acquisisca i dati personali tramite un sito web allocato in un server di un Paese extracomunitario che tratti, quindi, i dati fuori dall'ambito di applicazione delle norme relative alla profilazione. In questo caso l'ignaro consumatore che, convinto di essere tutelato, fornisse i propri dati personali spontaneamente, compilando magari un *form* su un sito web internet o, peggio ancora, che collegandosi al sito web i suoi dati venissero trafugati, rischierebbe di trovarsi "scoperto" dalla tutela delle norme prescritte per la profilazione. I sui dati potrebbero essere addirittura oggetto di commercio o essere trattati senza alcuna cautela.

Certo questi potrebbe intentare un'azione giudiziaria per gli eventuali illeciti penali e le violazioni amministrative commesse dall'azienda extracomunitaria, ma incontrerebbe non poche difficoltà: primo fra tutti l'individuazione dell'organo giudiziario competente, passando poi alla difficile (se non impossibile) applicazione delle azioni sanzionatorie dell'Autorità Garante per la protezione dei dati personali, fino ad arrivare (in alcuni casi) nella illegittimità ad agire nei confronti degli abusi per mancanza di applicazione della norma italiana.

Questo denota come spesso, soprattutto nell' "era digitale", le norme da sole non sono in grado di garantire una adeguata tutela da eventuali abusi della privacy.

6. *Fides supremum rerum umanarum vinculum*.

Molte aziende non affrontano adeguatamente il problema della privacy dei clienti, concentrandosi spesso su aspetti esclusivamente legali, piuttosto che sui benefici che la tutela della riservatezza genera per l'azienda, non rendendosi conto che un'adeguata tutela della privacy conferirebbe un rafforzamento del rapporto fiduciario con il cliente/consumatore, con conseguente aumento della domanda di mercato, miglioramento del tasso di risposta e rafforzamento dell'immagine aziendale.

---

sito, alle ipotesi di cui agli artt. 615-ter (eventualmente aggravato, ai sensi del comma 2, n. 3) o 615-quinquies (eventualmente in concorso col reato di cui all'art. 635-bis) del codice penale.

[29] Il provvedimento non ottemperato dal titolare potrebbe per es. quello di blocco del trattamento ottenuto dopo reclamo o ricorso al Garante esperito vittoriosamente dall'interessato.

In questa nuova ottica sarà fondamentale, quindi, che "il mercato" mostri la volontà al cambiamento non solo nella ricerca dell'attuazione puntuale della norma, ma soprattutto interpretando la questione con una visione etica del problema, predisponendo ad. es. norme di autoregolamentazione (c.d. codici etici), di modo che la fidelizzazione del consumatore si consolidi su questo nuovo modo di instaurare e intendere il "rapporto fiduciario".

Certamente questo obiettivo di cambiamento incontra la resistenza delle imprese che percepiscono tale mutamento esclusivamente come un onere eccessivo, sia dal punto di vista dell'organizzazione che da quello dei costi, ma è appropriato rilevare come il rispetto dell'etica d'impresa, per quanto oneroso possa essere, diventa sempre più parte di una strategia di comunicazione aziendale vincente, decisiva per lo sviluppo della comunicazione dell'imprese, soprattutto in ambito *on-line*.

In questa ottica orientata sulla correttezza e la trasparenza, la privacy dovrebbe diventare per "l'azienda" il perno fondamentale su cui fondare il "vincolo" che le consenta di fidelizzare i propri clienti.

* * *

«Il dubbio o la fiducia che hai nel prossimo sono strettamente connessi con i dubbi e la fiducia che hai in te stesso. (*Kahlil Gibran)*