

ROSANNA DE MEO

## AUTODETERMINAZIONE E CONSENSO NELLA PROFILAZIONE DEI DATI PERSONALI

**SOMMARIO:** 1. La profilazione e il trattamento dei dati personali. — 2. La profilazione nei provvedimenti del Garante della *privacy*. Breve repertorio. — 3. Trasparenza, libertà del consenso, proporzionalità del trattamento. — 4. La creazione di profili mediante l'arricchimento dei dati per aggregazione. — 5. La *policy* europea sulla protezione dei dati personali e sulla profilazione. — 6. Il consenso alla profilazione e il potere di autodeterminazione dell'interessato.

Una delle nuove frontiere del trattamento dei dati personali è rappresentata dallo studio dei comportamenti dei soggetti per tracciarne un profilo al quale ispirare campagne pubblicitarie, tecniche di *marketing*, decisioni relative all'accesso ad un servizio pubblico o privato. Il procedimento di raccolta di informazioni personali e comportamentali sfocia, poi, nella profilazione. Essa consiste in una tecnica di trattamento automatico, mediante algoritmi, di dati relativi a quantità numericamente anche molto elevate di persone, per attribuire a ciascuna di esse un profilo, cioè una categoria predefinita e delineata attraverso parametri che il responsabile del trattamento considera necessari alla sua ricerca, al raggiungimento del suo scopo. Il *target* è studiato nelle sue abitudini di consumo e negli stili di vita che ne rivelano attitudine e capacità di spesa, gusti per alcuni prodotti o servizi e disinteresse per altri, caratteristiche legate alla sua identità personale.

### 1. LA PROFILAZIONE E IL TRATTAMENTO DEI DATI PERSONALI.

La tecnica della profilazione è adottata prevalentemente — ma non esclusivamente — nel campo delle attività commerciali. Attraverso essa, infatti, la pubblicità potenzia la sua efficacia mediante la selezione del *target* al quale dirigere ogni singola campagna promozionale, differenziandola di volta in volta in relazione ai diversi profili creati in funzione degli obiettivi di mercato. Così, la *réclame* non è più diretta ad una generalità

\* Il presente scritto è stato preventivamente sottoposto a referaggio anonimo affidato a un componente il Comitato

Scientifico dei Referenti della Rivista secondo le correnti prassi nella comunità dei giuristi.

indistinta di consumatori o, nella migliore delle ipotesi, ad ampie categorie di soggetti individuate solo per età, genere o fasce socioeconomiche. L'analisi delle informazioni complesse ottenute dall'aggregazione automatica dei dati raccolti permette di strutturare le campagne sui comportamenti, sulle abitudini esistenziali delle persone studiate, in relazione ai diversi profili nei quali esse sono collocate, per rendere maggiormente invitanti i prodotti offerti.

Certo, il fenomeno non è nuovo<sup>1</sup>. La tecnica di analisi del mercato comincia, in particolare, quando i produttori e i distributori di beni e servizi di consumo, con l'obiettivo di fidelizzare la clientela, offrono promozioni, piccoli vantaggi e agevolazioni per ottenere le quali il consumatore è indotto a fornire i dati personali, spesso anche anagrafici, che lo riguardano<sup>2</sup>. La mole delle informazioni ottenute diviene una ricca miniera quando la si incrocia con le tracce lasciate dal consumatore con i suoi strumenti elettronici di pagamento e con le carte di fidelizzazione<sup>3</sup>. Si realizza, infatti, un'associazione immediata tra i dati identificativi e i dati di consumo. Non si tratta di poco: le abitudini alimentari, in particolare, possono tradire le convinzioni religiose (in alcuni periodi non sia acquista carne o carne di maiale), la presenza di alcune patologie (l'uso di alimenti privi di sostanze che danno intolleranze), la possibile composizione del nucleo familiare (anche se ci sono animali in casa) e, soprattutto, la capacità economica<sup>4</sup>. Se, poi, presso lo stesso grande distributore avviene l'acquisto di li-

<sup>1</sup> Vedi lo studio di J.I. RICHARDS, *Deceptive Advertising. Behavioural Study of a Legal Concept*, Hillsdale, New Jersey, 1990, 28 ss., il quale considera il fatto che quanto più le tecniche pubblicitarie si avvicinano alle abitudini e ai comportamenti dei consumatori (*getting inside consumers minds*), tanto più esse riescono a scongiurare il rischio di incorrere nel divieto che colpisce l'ingannevolezza della pubblicità ottenendo, però, l'effetto di avere maggiore presa sul convincimento dei clienti studiati.

<sup>2</sup> Le dimensioni raggiunte dal fenomeno hanno indotto il Garante per la protezione dei dati personali a stabilire alcune regole di comportamento alle quali i titolari del trattamento devono attenersi per garantire la liceità della loro attività e per ottenere le necessarie autorizzazioni dell'Autorità. Si tratta del provvedimento del 24 febbraio 2005, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web 1103045, nel quale si precisa come la profilazione debba rispettare criteri di anonimato per evitare «una relazione tra i dati che permettono di individuare gli interessati e le indicazioni analitiche relative alla loro sfera personale». Nei casi in cui non si possa garantire l'anonimato, la profilazione deve osservare il principio di proporzionalità, di pertinenza e di non eccedenza rispetto alle finalità commerciali rappresentate al cliente.

<sup>3</sup> Nel provvedimento del Garante per

la protezione dei dati personali del 19 novembre 2004, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web 1102815, si pone il caso del cliente che, per ottenere la carta di raccolta punti fedeltà da parte di un'azienda della quale era cliente, aveva comunicato il suo indirizzo esponendosi, così, alla ricezione indesiderata di messaggi promozionali. In quel caso, il Garante ha osservato come l'invio di pubblicità esulasse dagli obiettivi di raccolta punti per cui la carta era stata rilasciata, precisando come le informazioni ottenute attraverso l'uso delle *fidelity cards* possano essere trattate solo per il raggiungimento delle finalità enunciate al cliente al momento della richiesta di consenso.

<sup>4</sup> La possibilità che responsabili di differenti raccolte dati, per finalità autonome legate all'espletamento delle proprie attività, possano incrociare i dati dei quali sono rispettivamente in possesso per potenziare la selezione della propria clientela è tutt'altro che fantasiosa. Si veda, in proposito, il provvedimento del Garante per la protezione dei dati personali del 4 maggio 2006, in [www.garanteprivacy.it](http://www.garanteprivacy.it), (doc. web n. 1302385), nel quale è stata dichiarata illecita e vietata la pratica di un gestore di servizi di telefonia di richiedere i dati anagrafici al potenziale cliente (tra i quali il codice fiscale) per incrociarli con quelli in possesso di una società di gestione di informazioni creditizie al fine di valutare

bri e quotidiani, la « lista della spesa » potrà suggerire qualcosa in merito alle opinioni politiche, filosofiche e, insomma, potrà fornire spunti di descrizione del consumatore dal punto di vista della sua cultura e del suo pensiero.

La profilazione — e gli evidenti problemi di tutela giuridica della *privacy* che essa determina — raggiunge livelli di ancora maggiore penetrazione per gli utenti dei c.d. *social media*, siti di *e-commerce*, *social networks*, *blogs*, motori di ricerca e, in generale, per i fruitori dei servizi di telefonia e di comunicazione elettronica<sup>5</sup>. Chi frequenta un *social network* o utilizza servizi di *cloud computing* offre al gestore un'ampia gamma di dati personali, quali l'età, il sesso, la residenza, la professione — e molto altro ancora — che ne rendono facile l'identificazione e la profilazione attraverso la tecnica di tracciamento realizzata dai *cookies*. Le nostre sessioni di navigazione internet saprebbero descrivere noi stessi, le nostre abitudini, amicizie, immagini, curiosità, anche più di un padre confessore<sup>6</sup>.

Pertanto, tali operazioni tecnologiche di raccolta possono essere compiute in modo facile, rapido e in molti casi senza che l'interessato ne abbia una precisa consapevolezza<sup>7</sup> o, quanto meno, una esatta percezione di quanto possa essere rischioso rilasciare informazioni sensibili destinate a rimanere nel « patrimonio informatico » del gestore anche per lungo tempo senza una reale conoscenza dell'uso che di essi se ne potrà fare e della destinazione che ne potrà derivare.

Uno studio della Commissione Europea<sup>8</sup> rileva come i cittadini dell'Unione abbiano la percezione dell'importanza della loro identità elettronica e un forte timore dell'utilizzo che i titolari della raccolta possano fare delle informazioni rilasciate. Nonostante ciò, l'uso delle tecnologie e la facilitazione che esse rendono agli utenti nella realizzazione delle attività e degli scambi quotidiani potenzia la propensione a rivelare informazioni sensi-

l'opportunità di stipulare contratti di somministrazione in abbonamento. La persona che prendeva contatti con il gestore di telefonia non era consapevole, perciò, di essere stato valutato in relazione alla propria solvibilità.

<sup>5</sup> Il Garante per la protezione dei dati personali è intervenuto, proprio in materia di profilazione degli utenti da parte dei gestori di servizi di telefonia e comunicazione elettronica, con un provvedimento del 25 giugno 2009 (consultabile in [www.garante-privacy.it](http://www.garante-privacy.it)) nel quale sono indicate precise prescrizioni di comportamento e di ottemperanza delle autorizzazioni da richiedersi alla stessa Autorità. In questo provvedimento, il Garante sottolinea come « la circostanza che un fornitore possa disporre e trattare, seppur su base aggregata, tali tipologie di dati, comporta la disponibilità di un patrimonio informativo che va ben al di là delle informazioni considerate singolarmente e relative a ciascun interessato ».

<sup>6</sup> Sul punto, vedi le riflessioni di A. MANTELLERO, *Si rafforza la tutela dei dati personali: data breach notification e limiti*

*alla profilazione mediante i cookies*, in questa *Rivista*, 2012, 781, in relazione alla necessità di contenere legislativamente le pratiche di tracciamento delle navigazioni internet imponendo ai gestori di realizzare forme di *cookies* non per *default* ma per espressa accettazione dell'utente secondo la tecnica dell'*opt-in*.

<sup>7</sup> È noto il caso, risolto in via transattiva (l'accordo può leggersi in [www.ftc.gov](http://www.ftc.gov)), dell'attività di indagine condotta dalla Federal Trade Commission nei confronti della Sears Holdings Management Corporation, in relazione alla pratica di profilazione occulta condotta dalla Società nei confronti dei propri clienti i quali, nel registrarsi ad una *community* presentata sulla *home page*, inoculavano inconsapevolmente sulla propria macchina un *software* di ricerca in grado di tracciare le sessioni di navigazione.

<sup>8</sup> COMMISSIONE EUROPEA, Special Eurobarometer 359, *Attitudes on Data Protection and Electronic Identity in the European Union*, in [http://ec.europa.eu/public\\_opinion/archives/leb\\_special\\_en.htm](http://ec.europa.eu/public_opinion/archives/leb_special_en.htm).

bili, biografiche o sociali, come se tale abitudine sia divenuta parte integrante e inevitabile della vita quotidiana. Anzi, sono gli stessi cybernauti a desiderare di sentirsi riconoscibili attraverso la loro identità virtuale, a costruirsi una *second life* elettronica, a darsi un *nickname* tanto identificativo del sé nella rete quanto lo sia il nome anagrafico nella realtà<sup>9</sup>. E proprio questo desiderio di esistenza e vitalità virtuale<sup>10</sup> affievolisce il senso critico dei soggetti rendendoli più disponibili a rilasciare le informazioni sensibili che li riguardano pur di avere accesso alla società della rete.

Le dimensioni del fenomeno sono decisamente larghe, al punto da interessare l'intera industria della pubblicità. Negli Stati Uniti la Federal Trade Commission ha da tempo posto sotto stretta osservazione le pratiche di profilazione per l'alto rischio di compromissione della *privacy* che da esse deriva<sup>11</sup>. Le associazioni professionali dell'industria dell'*advertising* hanno così deciso di adottare un codice di autoregolamentazione nel quale si impegnano a osservare comportamenti di protezione verso il consumatore e l'utente nell'esercizio delle pratiche di profilazione<sup>12</sup>. In particolare, si assicura il massimo controllo sulle informazioni raccolte, e si assume l'impegno deontologico di attuare gli accorgimenti tecnologici diretti alla protezione fisica, elettronica e amministrativa dei dati trattati. Altrettanto importante, inoltre, è l'impegno alla conservazione delle raccolte per un tempo limitato, circoscritto in periodi brevi strettamente necessari alla realizzazione delle campagne alle quali il trattamento è diretto. Si propongono, inoltre, comportamenti etici diretti all'educazione del consumatore, per creare in lui la piena consapevolezza del valore del suo consenso alle pratiche di profilazione.

L'attenzione da parte del diritto di cui la profilazione necessita appare ancora più imprescindibile se si riflette sul fatto che tale tecnica di trattamento automatizzato può essere effettuata anche in altri contesti sociali — diversi rispetto a quelli della pubblicità commerciale — predisposti, per le funzioni istituzionali da essi svolte, a raccogliere direttamente ovvero ad avere accesso a raccolte di dati molto ampie e, al contempo, a presiedere all'erogazione di servizi pubblici che incrociano la vita e i diritti delle persone.

L'*e-government* ha aperto la strada alla raccolta di dati da parte di pubbliche amministrazioni, aziende sanitarie, agenzie, operatori finanziari e, in generale, esercenti di pubblici servizi che sono, così, in grado di racco-

<sup>9</sup> Si fanno sempre più forti le voci che intendono riconoscere, nell'accesso ad internet, un autonomo diritto fondamentale, specifico rispetto a quelli della realizzazione della personalità e della libera manifestazione del pensiero perché, in grado di richiedere una peculiare tutela di rango costituzionale: sul punto G. AZZARITI, *Internet e Costituzione*, in *Politica del diritto*, 2011, 374 s. e S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 386.

<sup>10</sup> Significative le parole di V. MATHIEU, *Privacy e dignità dell'uomo. Una teoria della persona*, Torino, 2004, 78, il quale descrive il fenomeno sottolineando come « il paradosso della tutela della per-

sona, nella situazione attuale, è che interesse delle persone non è solo che vengano divulgate informazioni il meno possibile, ma anche, all'opposto, che ne vengano divulgate il più possibile. Infatti, diventando virtuale il modo d'essere stesso della persona, questa non "esiste" se non in virtù della notizia che se ne ha ».

<sup>11</sup> In merito i riferimenti di S. STABILE, *Le nuove frontiere della pubblicità e del marketing su internet*, in *Dir. ind.*, 2009, 482 ss.

<sup>12</sup> Cfr. FEDERAL TRADE COMMISSION STAFF REPORT, *Self-Regulatory Principle for Online Behavioral Advertising*, in [www.ftc.gov](http://www.ftc.gov).

gliere, conservare ed elaborare informazioni sensibili, sociali e comportamentali particolarmente eloquenti e rivelatrici nell'utilizzazione a scopo di profilazione. Quanto più le informazioni raccolte si riferiscano a gruppi di persone estesi e definiti secondo criteri di appartenenza o riferibilità sociale, tanto più la profilazione lascia le dimensioni individuali per divenire profilazione di massa, possibile strumento di controllo della popolazione. Nei casi in cui queste categorie di enti pubblici e istituzioni, responsabili del trattamento, siano in grado di permettere o impedire l'accesso del soggetto a beni e servizi essenziali, la profilazione potrebbe trovarsi a svolgere un ruolo nel condizionare tali decisioni in maniera discriminatoria, lesiva di diritti fondamentali dei soggetti che subiscono la discriminazione in funzione della loro inclusione o esclusione dal profilo di riferimento. Sul punto, l'art. 14 del Codice della *privacy* esprime un preciso divieto al compimento di atti o provvedimenti giudiziari e amministrativi fondati sulla profilazione automatizzata.

Eppure, il frammentario interesse riservato dall'ordinamento al dilagare della profilazione nelle attività economiche e sociali — come meglio si avrà modo di esaminare nelle successive analisi — induce a riflettere sull'inadeguatezza della limitata tutela rimessa alla sola iniziativa di opposizione degli interessati. Riconoscere ai soggetti profilati un potere di controllo sui dati trattati può di per sé solo metterli al riparo dalle ingerenze dei responsabili del trattamento automatizzato?

La sensibilità dell'argomento risalta ancor più se si osserva come siano proprio gli operatori economici che realizzano attività di profilazione a proporsi quali garanti del rispetto dei diritti delle persone attraverso regole di deontologia che essi stessi si danno. L'alacre intervento dei grandi operatori delle attività di raccolta dati — i c.d. *big data*<sup>13</sup> — nel dotarsi di norme di autoregolamentazione induce a considerare che alla ricerca di un dichiarato comportamento deontologicamente corretto corrisponda un concreto interesse a voler presiedere alla formazione delle regole da seguire. Con ciò non si intende criticare *tout court* la funzione etica che le regole di deontologia assolvono in questo campo. È vero, però, che anche l'autoregolamentazione, così come tutti i processi di formazione di norme giuridiche<sup>14</sup>, necessita di proposizioni che non siano solo autoreferenziali ma che tengano buon conto delle istanze di tutela che si sollevano dalle persone coinvolte, per i loro interessi e diritti<sup>15</sup>. L'efficacia di una normazione

<sup>13</sup> A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in questa *Rivista*, 2012, 135 ss., considera come il potere informativo detenuto da pochi soggetti « differisce dalla semplice capacità di profilazione o di schedatura di massa, a cui hanno sempre guardato le norme in materia di *data protection*. Nel caso dei *big data* emerge infatti una nuova ed ulteriore valenza (...) la capacità predittiva che le analisi condotte con strumenti sofisticati su tali grandi aggregazioni possono conseguire ».

<sup>14</sup> Sulla produzione normativa extra-legislativa operata dai codici deontologici vedi G. PIEPOLI, *Autodisciplina professio-*

*nale e codici deontologici*, in AA.Vv., *Scritti in memoria di Pietro De Vecchis*, Roma, 1999, 767 ss., il quale legge nello spazio normativo lasciato all'autoregolamentazione « un disegno che mira ad un'integrazione della società mediante processi di autonomia sociale, istituzionalizzati e disciplinati dallo Stato, riducendo le aree del diritto legale e allargando corrispondentemente gli spazi del diritto extralegislativo prodotto dall'autonomia sociale ».

<sup>15</sup> L. MENGONI, *La questione del « diritto giusto » nella società post-liberale*, in *Rel. ind.*, 1988, 24, vede nell'autoregolamentazione una vocazione alla creazione di norme più vicine alla complessità degli interessi sociali: « è un nuovo tipo di *self-*

si misura proprio dalla capacità di essere risolutiva dei possibili contrasti fra interessi confliggenti e, perciò, alla *self-regulation* dei *big data* è giusto chiedere che essa si compenetri completamente nel possibile panorama di situazioni sensibili rispetto alla profilazione. Occorre verificare, infatti, che l'autodisciplina sia in grado non solo di conformare l'attività al raggiungimento del consenso degli interessati, ma che la sua protezione giuridica si spinga sino al punto di limitare, impedire, vietare la profilazione quando essa sia anche solo ipoteticamente compromissiva di situazioni giuridiche a tutela della persona e della sua dignità. È legittimo, perciò, porsi un serio interrogativo sull'efficienza di un sistema normativo che sia in larga parte demandato dalla *soft law* alla buona volontà dei tecnocrati<sup>16</sup> e che covi in sé il rischio — anche solo ipotetico — di non rappresentare tutte le categorie di interessi coinvolte.

L'analisi e le brevi considerazioni che seguiranno hanno l'obiettivo di avvalorare l'idea secondo la quale l'attività di profilazione merita un'osservazione diversa e specifica da parte del diritto, in funzione della caratteristica, propria di tale tecnica, di coinvolgere situazioni giuridiche che vanno oltre la compromissione della *privacy* — pur di per sé grave — per investire altri diritti legati alle libertà fondamentali<sup>17</sup>.

## 2. LA PROFILAZIONE NEI PROVVEDIMENTI DEL GARANTE DELLA *PRIVACY*. BREVE REPERTORIO.

La ricerca di una disciplina della profilazione dei dati personali trova nei provvedimenti dell'Autorità garante per la protezione dei dati personali (di seguito Garante) un primo importante *step* di considerazione. Infatti, questa peculiare tecnica di raccolta e trattamento è per nulla sconosciuta alla casistica dell'Autorità la quale, basandosi sulle norme del Codice della *privacy* e, in particolare, sulle competenze che le sono riservate, si è spesso imbattuta nella necessità di autorizzare preventivamente, disciplinare o dichiarare illecite le attività che siano del tutto o parzialmente basate su tecniche di profilazione.

Il Codice della *privacy* fa riferimento alla creazione e all'utilizzo di profili nel suo art. 14, esprimendo un preciso divieto nel caso in cui essi siano utilizzati per l'adozione di provvedimenti amministrativi o giudiziari fondati sulla valutazione dell'interessato attraverso la sua inclusione in un profilo creato per mezzo dell'elaborazione elettronica delle informazioni raccolte<sup>18</sup>. L'attenzione verso la peculiare rischiosità insita nel trattamento

*restraint* del diritto dello Stato, cioè un tipo di intervento non più diretto ma indiretto, indirizzato non a regolare con norme rigide e particolareggiate di comportamento i rapporti socio-economici, ma piuttosto a predisporre le nervature istituzionali di processi di autoregolamentazione sociale, a definire, correggere e ridefinire, quando occorra, istituzioni sociali funzionanti come sistemi autoregolatori ».

<sup>16</sup> S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, 36.

<sup>17</sup> Sul punto, le recenti considerazioni di S. RODOTÀ, *Il diritto di avere diritti*, op. cit., il quale rileva come le tecniche di profilazione possano incidere sul diritto fondamentale della persona alla dignità.

<sup>18</sup> Vedi L. BOZZI, *Le regole generali per il trattamento dei dati*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, 98 s., la quale rileva la chiara pericolosità dell'utilizzo dei profili automatizzati a fini decisionali ed esamina criti-

automatizzato dei dati confluisce, poi, nell'imposizione, a norma dell'art. 17, di una verifica del Garante preliminare all'inizio del trattamento<sup>19</sup>. Dal combinato disposto di queste due norme, perciò, si può individuare nei provvedimenti di autorizzazione preliminare — adottati *ex art.* 37 del Codice della *privacy* — il raggio di intervento all'interno del quale il Garante ha la possibilità di imporre delle condizioni all'esecuzione della profilazione, in chiave di garanzia per i diritti, le libertà fondamentali e la dignità dei profilati. E non solo. I poteri sanzionatori e normativi del Garante determinano, in alcuni casi, provvedimenti che hanno una *vis* di disciplina che va oltre la preliminare verifica di liceità, ma che ricerca e propone essa stessa le condizioni alle quali i titolari del trattamento devono improntare le loro attività.

Nei provvedimenti del Garante, il lettore ha la possibilità di individuare la tecnica del giurista che interpreta ed applica le norme esistenti per disciplinare un fenomeno che presenti elementi di peculiarità rispetto ai conflitti di interessi per i quali la disciplina generale era stata originariamente pensata. In alcuni interventi, ad esempio, il Garante si fa promotore di indagini su tecniche di trattamento estese in intere aree economiche e giunge a delineare le regole che serviranno agli operatori (per conferire liceità al loro operato) e agli interpreti (per valutare le eventuali condotte illecite). Si riscontra, in particolare, la tensione ad individuare soluzioni destinate a ripetersi nella casistica, pur se adattate alle diverse estrinsecazioni delle vicende da regolare.

Si può dire, in generale, che il Garante tende sempre nelle sue decisioni a realizzare una concreta attuazione del generale principio del consenso del titolare dei dati. In particolare, il trattamento è autorizzato solo quando si accerti che si sia data la concreta possibilità all'interessato di formarsi la precisa consapevolezza del fatto che la profilazione sarà un momento di ulteriore elaborazione dati, peculiare e distinto rispetto alla raccolta. Dall'esame dei provvedimenti si possono trarre degli orientamenti sui quali il Garante sembra improntare la sua concezione di liceità della profilazione. Essa, è pur vero, rappresenta un'attività ad alto rischio di compromissione della *privacy*, ma se esercitata secondo alcuni rigorosi parametri che garantiscano il pieno consenso e la libertà di scelta dell'interessato, essa può essere ritenuta legittima. In questo senso, la liceità dell'attività di profilazione deve essere riconosciuta solo in funzione della esatta conoscenza — fornita in termini di chiarezza all'interessato — dell'intenzione « profilatoria » di chi raccoglie i dati e palesemente dichiara le finalità che intende perseguire attraverso la profilazione. Il consenso dell'interessato deve essere specificamente rilasciato, a testimonianza della sua piena consapevolezza del fatto che dalle informazioni che lo riguardano sarà tratto un profilo che gli sarà attribuito. La libertà del consenso è testimoniata, ancora, dal fatto che quest'ultimo non sia considerato quale pre-condizione necessaria per l'accesso a servizi o *benefits*.

Pienezza della conoscenza, libertà e specificità del consenso sono, perciò, le regole generali elaborate dal Garante della *privacy* per disciplinare

camente la possibilità di profilazione riconosciuta in ambito privato osservando come « proprio le decisioni private sono le più frequenti e spesso più significative e pregiudizievoli per il cittadino ».

<sup>19</sup> Sul punto, E. PELLECCIA, *Art. 17 (Limiti all'utilizzabilità di dati personali)*, in *Tutela della privacy (Commentario alla legge n. 675/1996)*, in *Nuove leggi civ. comm.*, 1999, 459 ss.

e, così, consentire o negare le pratiche di profilazione. Nei successivi paragrafi prenderemo in esame alcuni provvedimenti, selezionati per argomenti omogenei, in quello che può leggersi come un breve quanto significativo repertorio.

### 3. TRASPARENZA, LIBERTÀ DEL CONSENSO, PROPORZIONALITÀ DEL TRATTAMENTO.

Ad una prima lettura, l'esame dei provvedimenti rende l'idea di come la profilazione abbia una prevalente — anche se non unica — contiguità con le attività di *marketing*. Spesso il Garante si è trovato a puntare l'attenzione sul fatto che la finalità di profilazione debba essere ben distinta dalle attività di *marketing* che possono essere dichiarate al momento della raccolta dei dati sia per attrarre il consenso dell'interessato a rilasciare le informazioni richieste e sia per coprire la stessa intenzione di profilare.

In un provvedimento diretto a regolare la fidelizzazione dei clienti mediante il rilascio di « carte »<sup>20</sup> — tipiche quelle di raccolta punti nella grande distribuzione — è possibile osservare come sia posta una specifica disciplina che, distinguendo la profilazione dall'attività di *fidelizzazione*, delinea con precisione le condizioni entro le quali la prima può essere considerata lecita. Dal punto di vista dell'operatore economico, la profilazione dei clienti può essere vista come elemento propulsore delle tecniche di *marketing*, perché conferisce una migliore conoscenza del *target* al quale indirizzare le campagne. Nell'ottica della tutela del consumatore, invece, le due diverse pratiche possono essere ben distinte in funzione del tipo di intromissione nella vita privata che da esse deriva.

Il provvedimento sulle *fidelity cards*, a questo proposito, distingue tra finalità di fidelizzazione in senso stretto e di profilazione. Nelle prime, il trattamento sulle informazioni anagrafiche e sul volume di spesa registrato sulla carta è finalizzato a determinare i premi, i *benefits* che il distributore riconosce al proprio cliente. In questo caso, il Garante dispone che « possono essere trattati esclusivamente i dati necessari per attribuire i vantaggi connessi all'utilizzo della carta » e il consenso a questo tipo di trattamento è rilasciato dal consumatore nel momento stesso dell'accettazione della carta<sup>21</sup>. La finalità di profilazione, invece, è evidentemente ulteriore e differente rispetto alla fidelizzazione. Ulteriore, perché l'operatore economico utilizza i dati raccolti con il rilascio e l'uso della carta per raccogliere informazioni sui singoli consumatori. Differenti, perché il consumatore potrebbe desiderare i vantaggi ottenuti con l'uso della carta ma, al contrario, avvertire come intrusivo e non gradito il fatto di sapersi studiato nelle proprie abitudini di consumo. In questo senso, il Garante elabora la regola per

<sup>20</sup> Provvedimento del 24 febbraio 2005, 'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1103045.

<sup>21</sup> Provvedimento 'Fidelity card', cit.: « per ottenere la carta di fidelizzazione e fruire dei relativi vantaggi occorre di rego-

la accettare condizioni generali di contratto predisposte dal titolare del trattamento (...) Poiché il trattamento di dati preordinati alla fidelizzazione in senso stretto è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato non è corretto, in questo caso, sollecitare il consenso al trattamento dei dati ».



la quale la liceità del trattamento per ogni finalità «altra» rispetto all'uso della carta è subordinata ad un consenso specifico, informato e distinto per ciascuna di esse. La necessità del consenso dell'interessato rappresenta, perciò, la misura della tutela giuridica a lui riservata rispetto al trattamento che l'operatore commerciale possa fare dei dati raccolti. In questa disposizione del Garante si ritrova, allora, un'attuazione del generale principio del consenso. Agli occhi dell'ordinamento, il consenso dell'interessato al trattamento dei dati che lo riguardano rappresenta lo strumento giuridico per riconoscere alla persona il controllo sulla propria identità e sulle informazioni che si intendono rivelare e far circolare su di sé. In applicazione di questa regola generale, le operazioni di trattamento dati per finalità di profilazione e *marketing* devono sempre ricevere legittimazione dal consenso dell'interessato.

Si può delineare, perciò, una specificazione fra le finalità di *marketing* e fidelizzazione rispetto alla profilazione. La linea di demarcazione fra tali finalità è segnata dal diverso tipo di intrusione sopportato dalla persona nella sua sfera privata. In questo senso, si registra l'attenzione del Garante per un preciso dovere di trasparenza del titolare del trattamento nei confronti della persona da profilare. Chi entra in contatto con proposte commerciali o campagne di promozione e pubblicità deve essere pienamente consapevole del preciso uso che si intende fare dei dati raccolti e, in particolare, deve essere specificamente informato del fatto che sarà tratto un profilo in base all'analisi di abitudini e scelte di consumo. Se ne trae la conseguenza di considerare illecite le schede contenenti condizioni generali e richieste di consenso dalle quali il sottoscrittore non possa trarre elementi per formarsi un pieno e consapevole convincimento, perché carenti di informative relative all'attività di profilazione e alle finalità con essa perseguite<sup>22</sup>. Il Garante osserva il profilo dell'informativa da rendere al momento del consenso non solo sul piano formalistico, ma su quello più decisivo della trasparenza. Non una semplice comunicazione, una generica *disclosure* magari inserita in un modulo di consenso denso di altre informazioni, può essere considerata adeguata a determinare una precisa consapevolezza nell'interessato. La trasparenza, invece, trova piena attuazione in funzione delle modalità con le quali l'informazione è data. Si può dire che il consenso sia pienamente formato solo quando l'intelligibilità, la formulazione, la stessa presentazione grafica con cui è espressa l'informativa rendono essa e il suo significato pienamente accessibile da chi consente al trattamento dei dati che lo riguardano<sup>23</sup>.

<sup>22</sup> Osserva in proposito il Garante (nel provvedimento *'Fidelity card'*, cit.) come «il rilascio delle carte (spesso preceduto dalla compilazione di un modulo di adesione e di questionario) e la loro utilizzazione (che determina la registrazione di acquisti di beni e servizi) comportano un trattamento dei dati personali dei clienti e, a volte, dei loro familiari. Accanto a dati anagrafici e recapiti sono spesso raccolte altre informazioni relative al cliente o ai suoi familiari non necessarie per attribuire i vantaggi collegati alla carta (titolo di studio, professione, interessi, abitudini, preferen-

ze, modalità di acquisti, ecc.). Tali informazioni vengono di frequente trattate unitariamente, per finalità diverse che richiedono quindi modalità differenziate; non di rado è fornita solo un'informativa generica che descrive i trattamenti in modo non adeguatamente distinto».

<sup>23</sup> In generale, sull'informativa vedi V. ZENO ZENCOVICH, Art. 10 (*Informazioni rese al momento della raccolta*), in E. GIANNANTONIO, M.G. LOSANO, V. ZENO ZENCOVICH (a cura di), *La tutela dei dati personali. Commentario alle legge 675/1996*, Padova, 1997, 95 ss.

La regola di trasparenza che impone una informativa chiara e specifica sulle finalità di profilazione, era destinata — per la sua caratteristica di generalità — ad andare oltre il confine del caso specifico delle *fidelity cards* e ad estendersi a molteplici casi di profilazione inconsapevole, nei quali i dati erano raccolti dichiaratamente per l'esecuzione di obblighi contrattuali ma occultamente sottoposti a profilazione. Così, è stata vietata la profilazione su dati personali e abitudini di consumo raccolti in occasione di rapporti fra professionisti e utenti di beni e servizi di varia natura, quali la fornitura energia elettrica<sup>24</sup>, la fruizione di strutture turistico-alberghiere<sup>25</sup>, la partecipazione a concorsi a premio via radio o web<sup>26</sup>, l'uso di servizi autostradali<sup>27</sup> e di trasporto<sup>28</sup>, l'accesso a servizi di *customer care*<sup>29</sup>. Il Garante, in particolare, si preoccupa di verificare che i *form* di consenso — sia cartacei sia elettronici — siano specifici per la finalità di profilazione, ben distinti rispetto ai moduli consenso per l'accettazione delle condizioni generali di contratto con le quali l'utente rilascia le informazioni necessarie al professionista per dare esecuzione alle prestazioni oggetto del rapporto contrattuale<sup>30</sup>.

<sup>24</sup> Provvedimento del 16 dicembre 2009, *No alla profilazione occulta*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1688999, nel quale è vietato al fornitore di energia « di utilizzare le dichiarazioni di consenso al trattamento dei dati già rilasciate dagli interessati per finalità di analisi delle abitudini e scelte di consumo dei clienti ».

<sup>25</sup> Provvedimento del 9 marzo 2006, *Profilazione della clientela di alberghi*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1252220, nel quale si dichiara illecito il trattamento profilatorio dei dati personali dei clienti associati alle informazioni relative alle loro abitudini, asseritamente raccolte per offrire migliori servizi.

<sup>26</sup> Provvedimento del 22 luglio 2010, *Concorsi online e web radio: no alla profilazione occulta*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1741988, nel quale per poter partecipare ad un gioco che metteva in palio una *compilation* musicale il fruitore doveva consentire al trattamento dei suoi dati anagrafici (es. età, sesso, professione) e dei suoi recapiti (es. residenza, telefono, mail) senza che fosse informato della possibilità di essere profilato.

<sup>27</sup> Provvedimento del 3 novembre 2005, *Telepass e libero consenso per finalità di marketing*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1195215, nel quale sono dichiarati irregolari i consensi prestati in occasione dell'esecuzione del servizio di telepass perché non specificavano all'utente la possibilità di essere profilato in relazione ai dati anagrafici, età, titolo di studio, tipo e targa di veicolo, ed altre « indicazioni di carattere generale sulle proprie caratteristiche, sugli interessi e sulla sua condizione economica ».

<sup>28</sup> Provvedimento del 5 marzo 2009, *Biglietti on line: il consenso all'uso dei dati non deve mai essere condizionato*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1615731, nel quale è vietato ad una società di biglietteria *on line* di conservare e profilare le informazioni relative all'acquirente del biglietto, raccolte elettronicamente al momento dell'acquisto (indirizzo IP, tipo di browser, identificativi delle sessioni di navigazione). Vedi, inoltre, l'analogo provvedimento 8 aprile 2010, *Marketing: necessario il consenso per l'invio di comunicazioni promozionali*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1721205, relativo ad un sito per l'acquisto *on line* di voli aerei, nel quale è richiesto un *form* specifico per il consenso alla profilazione a alle proposte di *marketing* via mail.

<sup>29</sup> Nel provvedimento del 15 novembre 2007, *Adempimenti semplificati per il customer care*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1462788, il Garante propone un *vademecum* per le attività di assistenza al cliente spesso fornite da soggetti pubblici o privati nello svolgimento delle proprie attività istituzionali, professionali, commerciali o di natura personale. In esso si prescrive all'operatore di *customer care* di dichiarare all'utente in maniera esplicita e specifica se le informazioni da egli rilasciate per ottenere l'assistenza richiesta saranno oggetto di profilazione.

<sup>30</sup> Provvedimento del 15 luglio 2010, *Raccolta di dati via internet per finalità promozionali: sempre necessario il consenso degli interessati*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1741998, nel quale si impone ad un sito di compravendite immobiliari di modificare il *form* di registrazione e

La necessità che il titolare dei dati possa formarsi un completo ed esatto convincimento circa il consenso da dare o negare alla richiesta di trattamento profilatorio è anche perseguita — oltre che con la prescrizione delle regole di trasparenza che abbiamo osservato — attraverso la dichiarazione di illiceità di quei trattamenti che siano ottenuti attraverso manifestazioni di consenso non pienamente libere da parte degli interessati, perché condizionate rispetto al raggiungimento dei vantaggi o delle prestazioni offerte dal professionista al momento della raccolta. Per usare i termini del Garante, il gestore deve dichiarare all'atto di costituzione del rapporto le eventuali finalità di profilazione e monitoraggio e chiederne il consenso senza «pressioni o condizionamenti», posto che «il conferimento dei dati e il consenso sono liberi e facoltativi rispetto all'ordinaria prestazione di servizi»<sup>31</sup>.

A questo proposito, è stato considerato non libero e, perciò, illecito il consenso prestato per le finalità di *marketing* e profilazione quando imposto nel *form* di adesione per ricevere i vantaggi promessi con la campagna di fidelizzazione, come se la manifestazione del consenso fosse la controprestazione alla quale fosse tenuto il cliente per poter ricevere i *benefits* reclamizzati<sup>32</sup>. Ancora, non è consentito al titolare del trattamento di «adottare comportamenti suscettibili di incidere sulle scelte libere e consapevoli» degli utenti, come l'induzione a «fornire informazioni personali senza aver avuto le spiegazioni e il tempo necessari per essere adeguatamente informati e maturare — allorché ciò è necessario — un consenso consapevole»<sup>33</sup>. È possibile notare, relativamente a questi provvedimenti, come la libertà di convincimento richiesta dal Garante quale parametro di liceità per i trattamenti di profilazione rispecchi pienamente l'orientamento già affermato con il «caso BNL»<sup>34</sup>, nel quale si affermava la necessità che il professionista non subordinasse i servizi da fornirsi al cliente rispetto al rilascio del consenso, come se quest'ultimo possa essere una controprestazione necessaria alla conclusione del contratto.

La lettura dei provvedimenti esaminati in questo breve repertorio, infine, rende conto di un ulteriore criterio di liceità richiesto per i trattamenti a scopo di profilazione: quello della proporzionalità fra informazioni

di accesso ai servizi perché preimpostato con un unico generico consenso al rilascio di informazioni con le quali il gestore del sito avrebbe elaborato studi e ricerche statistiche sugli orientamenti e le preferenze dell'utente. Vedi, altresì, il provvedimento 10 novembre 2010, *Tessera del tifoso: più garanzie per i supporters*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1779725, nel quale si specifica che le società calcistiche devono specificare, ai tifosi richiedenti le tessere elettroniche, le eventuali finalità di profilazione e raccogliere il loro consenso che, peraltro, non deve essere condizionato al rilascio della tessera.

<sup>31</sup> Provvedimento del 3 febbraio 2005, *TV interattiva: misure necessarie ed opportune per un trattamento dei dati conforme alle disposizioni vigenti*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1109503, nel quale il Garante formula delle prescrizioni

ai gestori di servizi televisivi interattivi, capaci di fornire un flusso informativo continuo, «che l'abbonato o l'utente trasmettono inconsapevolmente, mediante il canale di ritorno», riguardanti gradimenti, gusti o preferenze.

<sup>32</sup> Provvedimento del 15 novembre 2007, *Trattamento dei dati personali e fidelizzazione della clientela*, in [www.garanteprivacy.it](http://www.garanteprivacy.it), doc. web n. 1466898, nel quale si impone al titolare del trattamento di riformulare l'informativa assicurando una libera manifestazione del consenso degli interessati, non condizionata e necessaria per ottenere i vantaggi della campagna.

<sup>33</sup> Provvedimento *TV interattiva*, cit.

<sup>34</sup> Sul punto V. ZENO ZENCOVICH, «Il consenso informato» e la «autodeterminazione informativa» nella prima decisione del Garante, in *Corr. Giur.*, 1997, 915 ss.

raccolte e finalità perseguite con il trattamento. Innanzitutto, il Garante pone la condizione che la profilazione avvenga rispettando il più possibile l'anonimato<sup>35</sup>, in relazione alle finalità che si intendono perseguire. Se, cioè, gli obiettivi del titolare del trattamento possono essere soddisfatti attraverso la creazione di profili anonimi, l'utilizzo di dati personali o identificativi risulta illecito perché non rispondente ai criteri di pertinenza e non eccedenza richiesti dall'art. 11 del Codice. Sotto questo aspetto, i provvedimenti sulle *fidelity cards*<sup>36</sup> e sulla TV interattiva<sup>37</sup> sono significativi in quanto recano un'elaborazione dei criteri di pertinenza e non eccedenza nel senso di individuare in essi un generale principio di proporzionalità nelle operazioni di trattamento dati applicabile anche alla profilazione. Essa, cioè, deve essere svolta attraverso la massima economia di accumulo e conservazione di informazioni. Proprio per questo motivo, il titolare del trattamento ha l'obbligo di individuare preventivamente e con trasparenza gli obiettivi per i quali crea i profili e deve adoperare questionari, cartacei o telematici, su informazioni strettamente necessarie al perseguimento delle finalità prefissate. Tutte le informazioni che non conferiscano al profilo la significatività necessaria e sufficiente al raggiungimento degli obiettivi dichiarati, non possono essere elettronicamente elaborate e nemmeno raccolte e conservate: il loro trattamento è illecito.

#### 4. LA CREAZIONE DI PROFILI MEDIANTE L'ARRICCHIMENTO DEI DATI PER AGGREGAZIONE.

L'esame degli interventi autorizzativi, sanzionatori e « normativi » del Garante della *privacy* non può terminare senza rivolgere l'attenzione a come la profilazione sia stata oggetto di valutazione giuridica nel settore economico dei servizi di comunicazione elettronica accessibili al pubblico che, per sua stessa natura, permette agli operatori di entrare in contatto con flussi di dati elevatissimi e, soprattutto, con diverse tipologie di informazioni. Emerge, proprio in questa materia, uno degli aspetti più critici della profilazione, un argomento particolarmente significativo della rischiosità di questa tecnica di trattamento automatizzato: quello dell'arric-

<sup>35</sup> Vedi il provvedimento *Trattamento dei dati personali*, cit., nel quale il Garante ordina la cancellazione o la copertura con l'anonimato relativamente a dati, quali la professione dell'interessato e dei suoi familiari, non necessari per l'attuazione del programma di fidelizzazione. Vedi, altresì, il provvedimento *Profilazione della clientela di alberghi*, cit., che ritiene lecito solo il trattamento profilatorio eseguito su dati coperti dall'anonimato.

<sup>36</sup> Nel provvedimento *Fidelity card*, cit., si prescrive che i sistemi informativi siano configurati in maniera da « ridurre al minimo l'utilizzo di informazioni relative a clienti identificabili » e che, soprattutto per le finalità di profilazione della clientela, si disponga di « dati anonimi o

non identificativi (ad esempio, un codice numerico), senza una relazione tra i dati che permettono di individuare gli interessati e le indicazioni analitiche relative alla loro sfera personale (...) Se la finalità può essere perseguita con tali modalità (specie per quanto riguarda la profilazione della clientela per categorie omogenee), non è lecito utilizzare — e tanto meno conservare — dati personali o identificativi ».

<sup>37</sup> Nel provvedimento *TV interattiva*, cit., si fa divieto ai gestori dei servizi televisivi di conservare i dati raccolti in occasione della fatturazione del servizio per successive profilazioni, anche accettate dall'utente con specifico consenso, a meno che i dati non siano resi anonimi.

chimento dei dati per aggregazione, in grado di combinare informazioni per ottenere i cosiddetti *clusters*, cioè categorie all'interno delle quali inserire individui e gruppi. Infatti, l'aspetto forse più delicato della profilazione consiste nella possibilità di associare dati per ottenere un profilo sempre più dettagliato, sempre più intrusivo<sup>38</sup>.

Il Garante, in proposito, ha emanato un provvedimento di carattere generale contenente precise prescrizioni ai fornitori di servizi di comunicazione elettronica su reti pubbliche, considerando come per questi operatori economici l'attività di profilazione su base aggregata comporti la disponibilità di un patrimonio informativo di dimensioni eccezionali<sup>39</sup>. È proprio l'aggregazione che rende l'attività di profilazione ancora più invasiva e, perciò, più pericolosa per la *privacy* dell'utente. I dati personali aggregati, infatti, derivano dall'associazione di più informazioni, contenute in una pluralità di sistemi e possono restare nella disponibilità del titolare del trattamento, il quale è tenuto a conservarli per esigenze gestionali relative alla sua attività e, in taluni casi, per specifica richiesta di legge. « Il rischio che può derivare all'interessato da tale trattamento » emerge « dalla profondità del livello di aggregazione impostato e dalle modalità tecniche con le quali viene effettuato il trattamento »<sup>40</sup>. Il Garante, perciò, impone una regola di *prior checking* in base alla quale i fornitori di servizi di comunicazione elettronica dovranno sempre ottenere l'autorizzazione di cui all'art. 17 del Codice, senza la quale la profilazione attraverso l'aggregazione di dati sarà considerata illecita.

Un recente provvedimento autorizzativo<sup>41</sup> si segnala, perché rende immediatamente l'idea al lettore di quanto, nella realtà, il trattamento profilatorio di dati arricchiti per aggregazione possa davvero funzionare come una lente d'ingrandimento su aspetti assolutamente sensibili per la vita degli individui. Osserviamo il fatto. KW S.p.A. è una società fornitrice di servizi di comunicazione elettronica accessibili al pubblico. Essa intende svolgere attività di profilazione dei propri utenti senza doverne acquisire il preventivo consenso. Così, in base agli artt. 17 e 24 del Codice della *privacy*, rivolge al Garante una formale richiesta di autorizzazione su verifica preliminare delle condizioni e delle circostanze nelle quali avverrà il trattamento. KW dichiara, in proposito, che la profilazione sarà elaborata attraverso un arricchimento del proprio *data base*, ottenuto incrociando ed associando alcuni dati personali degli utenti (già patrimonio informativo della società, perché raccolti in occasione dell'esecuzione dei rapporti contrattuali di servizio) con nuove informazioni derivanti dall'elaborazione statistica di dati di natura geografica, socio-demografica, economica della popolazione presente nel relativo luogo di residenza. L'arricchimento sarà

<sup>38</sup> Osserva E. NAVARRETTA, Art. 9 (modalità di raccolta e requisiti dei dati), in *Tutela della privacy*, cit., 336, come « il singolo dato, rispetto all'identità personale, è come la tessera di un complesso mosaico, la cui costruzione, affidata alla mente dell'operatore e alle connessioni informatiche, può facilmente sfuggire allo specchio della realtà ».

<sup>39</sup> Provvedimento del 25 giugno 2009, *Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al publi-*

*co, che svolgono attività di profilazione*, in *www.garanteprivacy.it*, doc. web n. 1629107.

<sup>40</sup> Provvedimento *Prescrizioni ai fornitori di servizi di comunicazione elettronica*, cit.

<sup>41</sup> Provvedimento del 15 marzo 2012, *Arricchimento dei dati personali della clientela nell'ambito dell'attività di profilazione*, in *www.garanteprivacy.it*, doc. web n. 1903026.

elaborato elettronicamente da un terzo soggetto, responsabile del trattamento, che metterà a disposizione un apposito *software* di sua proprietà (denominato HJ) in grado di associare i dati della clientela di KW con quelli dell'indicatore geografico più piccolo del censimento Istat, consistente in una microzona di residenza di una cinquantina di famiglie. «Le famiglie inserite all'interno di HJ vengono categorizzate in funzione di specifici parametri quali: 1) le caratteristiche socio-demografiche della popolazione residente nella sezione (sesso ed età della popolazione, stato civile, titolo di studio, occupazione); 2) la struttura del nucleo familiare; 3) la capacità di spesa della famiglia; 4) la tipologia dell'unità abitativa; 5) le etnie straniere residenti»<sup>42</sup>. Come si può facilmente considerare, l'arricchimento dei dati proposto all'autorizzazione del Garante riuscirebbe ad ottenere un *cluster* davvero molto dettagliato su aspetti sensibili della vita dei soggetti profilati. Con il medesimo sistema, KW intende profilare anche i propri utenti professionisti, mediante l'arricchimento dei dati di cui essa dispone con quelli del software HJ che abbinano l'utente ad una determinata area geografica ad alla categoria merceologica di appartenenza.

Veniamo, ora, alle disposizioni del Garante il quale, pur autorizzando le operazioni del trattamento proposto, indica dei precisi parametri entro i quali dovrà avvenire la profilazione. Anche in questo caso, i profili di liceità del trattamento sono riconducibili al rispetto delle regole di trasparenza e proporzionalità che già in passato, come visto, il Garante ha elaborato applicando le disposizioni del Codice della *privacy* alla profilazione.

Innanzitutto, KW dovrà improntare il suo trattamento ad una peculiare regola di trasparenza che il Garante specifica nell'obbligo di rendere una chiara informativa agli interessati, pur avvalendosi dell'esonero dal consenso<sup>43</sup>. L'informazione agli interessati dell'esistenza di una profilazione che li riguarda, infatti, permette a costoro di poter esercitare il diritto di accesso e di controllo sui propri dati personali di cui all'art. 7 del Codice. Se è vero che KW potrà eseguire il trattamento senza il consenso dell'utente, a quest'ultimo deve essere riconosciuta la possibilità di controllare l'esistenza dei propri dati e di chiederne la cancellazione.

Si tratta, a ben guardare, di una applicazione della regola della trasparenza differente rispetto a quelle esaminate nel paragrafo precedente. In questo caso, infatti, la legittimazione alla profilazione non riposa sul consenso dell'interessato, ma sull'autorizzazione preventiva del Garante. L'informativa, perciò, non influisce sulla formazione del consenso alla profilazione ma sull'eventuale decisione della persona profilata di sottrarsi al trattamento. Alla persona non è data la possibilità di accettare la profilazione, prima che essa abbia inizio. L'interessato può solo rifiutarla e cancellarne i risultati quando essa sia già in atto, attraverso l'esercizio dei diritti riconosciuti dall'art. 7 del Codice della *privacy*.

<sup>42</sup> Sono le stesse parole usate dal Garante nel provvedimento *Arricchimento dei dati personali*, cit.

<sup>43</sup> Il provvedimento *Arricchimento dei dati personali*, cit., dispone in proposito che «alla luce del nuovo trattamento di arricchimento (...) di profilazione, la società dovrà modificare l'informativa che attualmente rende ai propri utenti richia-

mando tale trattamento e le relative caratteristiche e rendendo edotti gli interessati che lo stesso viene realizzato attraverso l'utilizzo di alcuni dati personali incrociati con altri dati di natura statistica, avvalendosi dell'esonero dal consenso (...) L'informativa dovrà essere modificata anche con riguardo all'esercizio dei diritti di cui all'art. 7 del Codice».

Inoltre, in ossequio alla regola della proporzionalità, il Garante verifica che la creazione dei *clusters* avvenga con la maggiore economia di dati possibile. In questo senso, se gli obiettivi della campagna promozionale di KW potranno essere raggiunti arricchendo i dati solo mediante l'aggregazione di parametri oggettivi (geografici e socio-demografici) di rilevazione statistica, il trattamento di informazioni di natura strettamente soggettiva (stato civile, etnia, titolo di studio e occupazione) dovrà essere evitato.

Significativa, a proposito del rispetto della regola della non eccedenza del trattamento rispetto agli obiettivi perseguiti, è l'imposizione di un termine di un anno per l'utilizzo dei dati, oltre il quale essi dovranno essere cancellati o resi anonimi. La limitazione temporale della conservazione dei dati aggregati, inoltre, offre maggiore sicurezza rispetto ad eventuali episodi di circolazione non autorizzata dei dati stessi.

## 5. LA POLICY EUROPEA SULLA PROTEZIONE DEI DATI PERSONALI E SULLA PROFILAZIONE.

Il diritto europeo conosce, nella tematica della protezione dei dati personali, una delle sue più alte espressioni di civiltà giuridica. Già con la Convenzione n. 108 del 28 gennaio 1981<sup>44</sup>, l'ordinamento europeo propone agli stati membri aderenti la necessità di disciplinare la materia secondo principi di liceità, consenso dell'interessato e accesso alla cancellazione o alla rettifica. In maniera più dettagliata, poi, la disciplina offerta dalla direttiva 95/46/CE<sup>45</sup> subordina l'interesse del mercato interno alla libera circolazione dei dati personali rispetto alla tutela del diritto fondamentale delle persone alla *privacy*. I principi ai quali l'impianto normativo si ispira, tra i quali quello della subordinazione della liceità del trattamento al consenso dell'interessato, sono confermati nelle diverse adozioni degli stati membri.

Eppure, evidentemente, l'evoluzione tecnologica così rapida e pervasiva ha prodotto profondi mutamenti dei comportamenti dei singoli o dei gruppi che siano produttivi di diffusione e suscettibili di raccolta ed elaborazione automatizzata. Vi sono perciò, tensioni continue del diritto<sup>46</sup> a raccogliere la sfida della tecnologia<sup>47</sup>, per disciplinare le pratiche di trattamento e raccolta, anche fraudolente o criminose<sup>48</sup>, rese possibili dalla nuove applicazioni elettroniche.

<sup>44</sup> Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, adottata a Strasburgo il 28 gennaio 1981 e ratificata in Italia con legge n. 98 del 21 febbraio 1989, in [www.privacy.it/convstrasb.html](http://www.privacy.it/convstrasb.html).

<sup>45</sup> In GUL 281 del 23 novembre 1995, 31 ss.

<sup>46</sup> G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in questa *Rivista*, 2012, 831 ss., osserva come la tecnica possa influenzare il diritto e viceversa: « il diritto dunque può influenzare lo sviluppo della tecnica, come è accaduto con la legislazione sulla firma digitale. La tecnica può

condizionare il diritto agevolando certe soluzioni (...) o addirittura fare diritto (*lex informatica*) ». Si vedano, inoltre, le importanti riflessioni sul rapporto fra diritto e tecnica scaturenti dal dibattito di N. IRTI e E. SEVERINO, *Le domande del giurista e le risposte del filosofo (dialogo su diritto e tecnica)*, in *Contratto e impresa*, 2006, 665 ss., che pongono il dilemma fra la tensione della tecnica a vivere delle sue stesse regole e la funzione del diritto di intervenire per limitarla con la sua disciplina.

<sup>47</sup> Così S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, 15.

<sup>48</sup> Vedi, in proposito, la Convenzione

Sull'argomento della profilazione, in particolare, la *policy* europea si è espressa sinora in maniera meno decisa. Si può segnalare in proposito un intervento di *soft law* recato dalla Raccomandazione del Comitato dei Ministri del 23 novembre 2010<sup>49</sup>, con la quale il Consiglio d'Europa enuncia le norme minime che gli stati membri dovrebbero avere come riferimento nell'adozione di provvedimenti normativi o di autoregolamentazione per la protezione della vita privata e dei diritti fondamentali nelle operazioni di profilazione.

Osservando l'impianto normativo della Raccomandazione si possono ritrovare in essa — sia pur maggiormente specificate — le stesse regole di liceità e correttezza già a grandi linee applicate nella casistica del Garante: il consenso dell'interessato deve essere libero, specifico e informato, senza che il responsabile possa subordinare l'accesso ai servizi al rilascio delle informazioni richieste; il consenso deve essere ottenuto al momento della raccolta e, ove ciò non sia previsto, il trattamento dovrà ritenersi lecito solo se si sia resa una piena ed efficace informativa idonea a permettere al titolare di esercitare i suoi diritti di accesso, rettifica e cancellazione; la profilazione deve avvenire per un limitato periodo temporale, mediante la raccolta e l'uso di dati adeguati, pertinenti e non eccedenti rispetto alle finalità proposte.

E importante, tuttavia, rilevare come la Raccomandazione proponga una disciplina dettagliata sulla correttezza dell'informativa da rendere all'interessato, a garanzia del fatto che essa non si risolva in un mero momento formalistico ma, invece, rappresenti la trasparenza necessaria per poter dire che il consenso si sia formato in piena consapevolezza. Essa, infatti, all'art. 4 indica una serie di specifiche informazioni da portare a conoscenza dell'interessato che, nel loro complesso, rappresentano una garanzia del fatto che il trattamento profilatorio avvenga in condizioni di massima trasparenza, così che l'interessato possa non solo comprendere bene in cosa si sostanzierà la profilazione e quali saranno le sue conseguenze<sup>50</sup> ma, in particolare, egli possa anche avere tutti i riferimenti specifici per poter interrompere in ogni momento il trattamento<sup>51</sup>. Le informazioni, allora, non possono mai essere generiche, ma devono essere in grado di sostenere l'autodeterminazione dell'interessato nel momento della formazione del consenso e nell'esercizio dei diritti di dissenso. A tal fine, infatti, la Raccomandazione propone una sorta di « *bill of rights* » a favore

sulla criminalità informatica del Consiglio d'Europa (ETS 185 - Convenzione di Budapest).

<sup>49</sup> Raccomandazione CM/Rec (2010) 13, sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione, in <https://wcd.coe.int>.

<sup>50</sup> L'art. 4 della Raccomandazione prescrive che l'interessato sia reso edotto non solo dell'intenzione di profilare i le informazioni che egli renderà ma, soprattutto, egli deve avere la possibilità di conoscere le finalità della profilazione e se i suoi dati potranno venire in contatto con soggetti diversi dal responsabile del tratta-

mento e per quali motivi. Importante, inoltre, è il riferimento della Raccomandazione all'informazione relativa all'eventuale rapporto esistente fra il rilascio delle informazioni e l'accesso ai servizi offerti nonché agli « effetti previsti dell'attribuzione del profilo al singolo interessato ».

<sup>51</sup> L'art. 4 della Raccomandazione indica, quali criterio di correttezza della profilazione, la necessità di informare l'interessato circa l'identità del titolare e del responsabile del trattamento, nonché « le categorie di persone o enti ai quali i dati personali possono essere comunicati » e « le persone o i soggetti presso i quali sono o saranno raccolti i dati ».



degli interessati, affinché a costoro sia assicurata la possibilità di intervenire in qualunque momento per sospendere la profilazione e per opporsi ai suoi effetti quando da essa derivino decisioni che possano avere « un impatto significativo sulla persona ».

La Raccomandazione rappresenta il primo testo internazionale che si interessi di individuare norme minime relative alla protezione della vita privata nell'ambito del trattamento automatizzato dei dati con finalità di profilazione. Le regole in essa contenute sono segnalate alla libera adozione delle legislazioni interne nonché alla buona volontà dell'autoregolamentazione degli operatori del settore. La scelta di intervenire attraverso un atto di *soft law* denuncia il desiderio dell'Unione di muoversi con delicatezza in un campo caratterizzato da interessi contrapposti<sup>52</sup>, rappresentati sia dalla rilevanza economica degli obiettivi del titolare del trattamento e sia dalla possibile compromissione dei diritti fondamentali delle persone profilate.

Il ricorso alla normazione di indirizzo mediante un provvedimento di *soft law* per l'introduzione di regole giuridiche da attualizzarsi attraverso le legislazioni interne o mediante i codici di condotta<sup>53</sup>, si giustifica anche se si pensa che le tecniche di profilazione possono assolvere a funzioni anche di beneficio per gli stessi soggetti profilati e della collettività, perché permettono l'analisi dell'economia e della società e consentono l'analisi e la prevenzione di rischi e frodi alla sicurezza. A questo proposito, infatti, la Raccomandazione riconosce agli Stati membri la possibilità di derogare alle regole del preventivo consenso e dell'informazione all'interessato quando la profilazione sia necessaria per motivi di sicurezza nazionale, pubblica o per la repressione dei reati, ponendo quale condizione di liceità la specifica previsione di legge<sup>54</sup>.

<sup>52</sup> F. CAFAGGI, *Social Norms, Self-regulation and the European Integration of Private Law: an Alternative Law and Economics Perspective*, in [www.eui.eu](http://www.eui.eu), secondo il quale « self-regulation is an alternative and/or complementary tool in the area of social policies. Self-regulation has been recognized expressly as a harmonization device in the area of media law. Explicit references concern for example privacy and electronic commerce. In other areas reference to self-regulation is explicit. For example false and comparative advertising ». In ogni caso, anche se legittimata, l'autoregolamentazione non è imposta ma suggerita attraverso atti non vincolanti.

<sup>53</sup> Il ricorso a strumenti di *self regulation* per l'individuazione di regole specifiche nei diversi settori socio economici che possano impattare con pratiche di trattamento di dati sensibili non è nuovo nella *policy* europea a tutela della riservatezza. Anzi, la direttiva 95/46/CE all'art. 27 è tra i primi atti comunitari a prevedere e, quindi, legittimare la sussidiarietà normativa dei codici di autodisciplina in forza della quale alle organizzazioni pri-

vate rappresentanti di categorie professionali o economiche è riconosciuta una maggiore adeguatezza nella disciplina del settore di competenza. Sul punto vedi S. SILEONI, *Autori delle proprie regole. I codici di condotta per il trattamento dei dati personali e il sistema delle fonti*, Padova, 2011, 131 s., secondo la quale « l'aver previsto in un atto comunitario vincolante l'utilizzo di un modello di autoregolamentazione equivale ad un riconoscimento, da parte del legislatore comunitario, di un loro rilievo nella disciplina di un diritto di rilevanza costituzionale, motivata dalla preferenza per uno strumento giuridico agile e appropriato ad una materia di alta tecnicità ».

<sup>54</sup> Art. 6: qualora ciò risulti necessario in una società democratica per motivi di sicurezza nazionale, sicurezza pubblica, per tutelare gli interessi dello Stato o per la prevenzione e repressione di reati penali, o per la tutela dell'interessato o delle libertà e diritti di terzi, gli Stati membri non sono tenuti ad applicare necessariamente le disposizioni (...) della presente raccomandazione, purché ciò sia previsto dalla legge.

Pur con la sua natura non vincolante, la Raccomandazione emerge per la caratteristica di offrire all'interprete l'indicazione dei possibili momenti di conflitto esistenti fra la profilazione e i diritti degli interessati, individuandone il campo elettivo nella tutela dei diritti fondamentali. Si coglie nel testo del provvedimento la concreta consapevolezza del fatto che la profilazione è in grado di compromettere diritti dell'uomo ulteriori rispetto a quello della *privacy*, legati alla possibilità di discriminazioni in base a profili costruiti in funzione del genere, dell'origine razziale o etnica, della religione e delle condizioni personali quali l'età, la salute o l'orientamento ideologico e sessuale<sup>55</sup>. La raccomandazione, infatti, ben individua la rischiosità della profilazione nella sua grande potenzialità predittiva relativamente a caratteristiche di personalità e di comportamento di individui e gruppi. E proprio tale caratteristica stimola l'interesse del diritto alla sua disciplina per evitare che, sulla base di semplici profili, le persone possano essere automaticamente oggetto di decisioni o vittime di discriminazioni e stigmatizzazioni sociali.

#### 6. IL CONSENSO ALLA PROFILAZIONE E IL POTERE DI AUTODETERMINAZIONE DELL'INTERESSATO.

Il problema della profilazione, che ne caratterizza la rischiosità in termini di tutela delle libertà fondamentali e della dignità non è solo nella raccolta e nel trattamento dei dati quanto, piuttosto, nell'attribuzione del profilo. Attraverso il trattamento automatizzato si crea il profilo, ma il rischio è che esso possa poi diventare una prigione, una veste stretta posta addosso all'interessato dalla quale possa derivare discriminazione e alterazione dell'identità con la quale egli si pone nei confronti di chi, in base a quel profilo, abbia la possibilità di decidere del suo accesso a servizi ai quali egli sia interessato.

Con la profilazione non si rischia solo il sacrosanto diritto di ognuno *to be let alone*.

Queste tecniche sono tanto più intrusive in quanto sono in grado di costringere il soggetto in un *cluster* ottenuto sulla base di dati elettronicamente generati. E non è soltanto una questione di verosimiglianza del profilo rispetto all'interessato al quale esso viene attribuito. Potrebbe anche darsi che il profilo creato dall'algoritmo corrisponda di fatto alla condizione personale attribuita all'interessato ma ciò può essere contrario al diritto della persona di autodeterminarsi nella scelta degli elementi di identità personale da divulgare<sup>56</sup>.

In altri termini, con la profilazione si ottiene una catalogazione delle persone che già di per sé si contrappone ai concetti di dignità, di libertà

<sup>55</sup> Osserva L. BOZZI, *Le regole generali per il trattamento dei dati*, cit., 98, come «l'elaborazione dei profili e la ricostruzione di personalità effettuate con mezzi automatizzati (...) presentano una lesività potenziale tale da trascendere la sfera della tutela della riservatezza e dell'identità personale dell'interessato per porsi sicura-

mente in una dimensione super o metaindividuale».

<sup>56</sup> In questosenso, il diritto alla *privacy* può essere efficacemente descritto come «il diritto di mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata», S. RODOTÀ, *Tecnologie e diritti*, cit., 202.

e di potere di controllo sulla propria identità personale. L'interessato che non desidera essere profilato non può accontentarsi di considerare che il profilo nel quale è stato rinchiuso corrisponde esattamente alle sue caratteristiche, perché egli ha l'interesse e il diritto a manifestare o a nascondere caratteristiche della sua identità in funzione della sua esclusiva volontà.

La casistica dimostra come la profilazione possa essere in sé lesiva della riservatezza e della dignità della persona perché il soggetto profilato perde il pieno controllo di quella parte di identità personale rivelata dal profilo. Pensiamo al tipo di profilazione valutata nel provvedimento *Arricchimento dei dati personali*: se abito in un quartiere degradato della città, perché dovrebbe saperlo il gestore della mia utenza di traffico dati? Pensiamo, ancora, al provvedimento *Profilazione della clientela di alberghi*: se i miei studi si sono fermati alle scuole dell'obbligo, perché il mio nome dovrebbe rimanere registrato nel cluster 'basso livello di istruzione' conservato nel *data base* dell'albergo nel quale ho dimorato durante le vacanze? Ricordiamo, infine, il provvedimento sulle *Fidelity card*: se sono stato profilato come 'economicamente benestante', perché ciò dovrebbe essere mantenuto negli archivi elettronici del produttore dei cosmetici di alta gamma di cui ho accettato in profumeria un campione gratuito? La risposta è facilmente comprensibile dal punto di vista delle imprese di settore. I trattamenti elettronici di profilazione e la loro particolare capacità predittiva potenziano fortemente la conoscenza e l'analisi del mercato e, con ciò, rispondono pienamente alla realizzazione degli interessi dell'economia della produzione di beni e servizi di massa<sup>57</sup>. Si comprende, allora, il motivo per cui gli interventi normativi in questa materia sono sempre molto cauti, anche in considerazione della connotazione multinazionale del fenomeno dovuta al fatto che i maggiori raccoglitori di dati elettronici sono dislocati in diverse parti del mondo ed hanno una tale capacità economica che consente loro di esercitare una importante influenza lobbistica.

Dall'angolo visuale dei diritti della persona, invece, la necessità di porre regole che contrappongano alla raccolta e alla profilazione di massa dei dati — soprattutto quelli elettronici generati dalla navigazione sulla rete — diviene ineludibile in funzione della sempre maggiore tutela che fonti normative multilivello riconoscono ai diritti fondamentali e, fra essi, alla protezione della sfera privata dell'individuo.

La continua evoluzione della tutela della riservatezza ha potenziato l'intervento degli ordinamenti nel riconoscere la capacità del singolo di governare la propria identità personale, soprattutto in relazione alle vicende di circolazione dei dati<sup>58</sup>. Il diritto alla *privacy*, ormai, deve essere declinato come diritto all'autodeterminazione della persona nel divulgare i propri dati<sup>59</sup>, come diritto di avere pieno controllo sulle caratteristiche di identità personale che gli altri percepiscono di noi<sup>60</sup> e di poter nascondere quanto

<sup>57</sup> A. MANTELERO, *Si rafforza la tutela dei dati personali*, cit., 786.

<sup>58</sup> G. PINO, *Teorie e dottrine dei diritti della personalità. Uno studio di meta-giurisprudenza analitica*, in *Materiale storia cult. giur.*, 2003, 237 ss.

<sup>59</sup> Osserva S. RODOTÀ, *Il diritto di avere diritti*, cit., 320, che «l'originaria definizione della privacy come "diritto di

essere lasciato solo" non è stata cancellata ma fa parte di un contesto via via arricchito da diversi punti di vista» quali il «controllare l'uso che gli altri fanno delle informazioni che mi riguardano», la «tutela delle scelte di vita contro ogni forma di controllo pubblico e di stigmatizzazione sociale».

<sup>60</sup> Sul diritto al controllo dei dati rela-

di sé non si desidera manifestare<sup>61</sup>, a meno che non esistano interessi superiori (magari di ordine pubblico o di sicurezza) al trattamento senza consenso.

Proprio nel riconoscimento della piena autodeterminazione dell'individuo sul proprio patrimonio informativo — rivelato o nascosto, esistente o potenziale — si può individuare un primo importante aspetto giuridicamente problematico della profilazione.

In base alle norme esistenti, la regola del consenso informato rappresenta il parametro di valutazione della liceità della profilazione. L'interessato che abbia ricevuto una corretta informazione sulle procedure di elaborazione elettronica alle quali saranno sottoposti i suoi dati legittima, con il suo consenso, il trattamento. In questo senso, la vigilanza del Garante in relazione alla trasparenza delle informazioni rese all'interessato al momento del consenso dimostra come la sequenza «informativa-conoscenza-consenso» tuteli il diritto della persona a non subire passivamente la profilazione. L'attenzione riservata alla correttezza dell'informativa dimostra vieppiù come la regola della trasparenza sia necessaria a presidio dell'autodeterminazione dell'interessato. Infatti, l'informativa è in grado di conferire liceità alla profilazione solo quando rende identificabile il soggetto responsabile del trattamento e le procedure necessarie affinché l'interessato possa esercitare il suo potere di controllo, rettifica e distruzione dei dati profilati.

In alcuni casi, però, come abbiamo visto, l'autorizzazione preventiva alla profilazione incide sulla sequenza «informativa-conoscenza-consenso» in quanto la liceità del trattamento riposa non sul consenso dell'interessato ma sulla semplice informativa in grado di poter formare la conoscenza circa l'esistenza di una profilazione dei dati. È quanto abbiamo potuto osservare nel provvedimento *Arricchimento dei dati personali*: la liceità del trattamento profilatorio ha trovato la sua causa giustificativa non già nel consenso degli interessati ma nell'autorizzazione unita alla prescrizione di un'informativa dettagliata. Il margine di intervento lasciato alle persone profilate a tutela della loro autodeterminazione è stato relegato al diritto di opposizione. La tutela degli interessati, posti a conoscenza dell'esistenza di un processo di profilazione nei loro riguardi, perde il carattere attivo della necessità del consenso per rimanere costretta nel più esiguo margine della resistenza, dell'opposizione.

Con l'autorizzazione preventiva, l'autodeterminazione dell'interessato non si traduce più nel potere di scegliere se accettare o meno di essere sot-

tivi all'identità personale, vedi *ex multis* V. ZENO ZENCOVICH, *Identità personale*, in *Dig. Disc. Priv.*, sez. civ., IX, Torino, 1993, 294 ss. e G. FINOCCHIARO, *Identità personale (diritto all')*, in *Dig. Disc. Priv.*, sez. civ., Agg., Torino, 2010, 722 ss.

<sup>61</sup> Sul diritto a non manifestare informazioni personali, molto importante è il riconoscimento del diritto all'oblio come controllo sull'identità personale. Sul punto, *ex multis*, M.R. MORELLI, *Oblio (diritto all')*, in *Enc. Dir.*, Agg. VI, Milano, 2002, 848 ss. In particolare, sul diritto all'oblio nella rete per governare l'immagine storica

che ognuno vuole presentare di sé, vedi M. MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009; G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in questa *Rivista*, 2010, 391 ss. e S. RODOTÀ, *Il diritto di avere diritti*, cit., 406, secondo il quale «il diritto all'oblio si presenta come diritto a governare la propria memoria, per restituire a ciascuno la libertà di reinventarsi, di costruire personalità e identità affrancandosi dalla tirannia di gabbie nelle quali una memoria onnipresente e totale vuole rinchiusare tutti».

toposti a profilazione bensì in una forma di autodifesa consistente, di volta in volta, nel chiedere l'accesso ai dati conservati dal responsabile del trattamento per pretenderne la modifica o la cancellazione. Le differenze non sono di poca rilevanza. L'interessato non potrà più esprimere il suo diniego nel momento del contatto con chi gli propone il trattamento ma dovrà attivarsi in seguito all'informativa per esercitare il suo diritto di opposizione. Si giunge, così, a chiedere all'interessato «una indeterminata serie di atti difensivi, mentre dall'altra parte i signori delle informazioni, già in condizioni di esercitare sugli utenti varie forme di pressione, possono limitarsi a una attesa che consente loro di beneficiare di una situazione che, per ragioni di tempo o di insufficiente informazione, induce alla passività»<sup>62</sup>.

Inoltre, si può considerare come, attraverso la previsione dell'autorizzazione preventiva, l'art. 14 del Codice legittima la possibilità che la profilazione possa preludere all'adozione di determinazioni di tipo contrattuale assunte verso l'interessato in funzione del profilo attribuito. Il divieto che ciò avvenga è forte per quanto riguarda gli atti o i provvedimenti di tipo giudiziario o amministrativo. La norma, invece, riserva una tutela meno forte all'interessato per quanto riguarda le decisioni assunte nella conclusione o nell'esecuzione di un contratto. Infatti, quando vi sia l'autorizzazione preventiva di cui all'art. 17 del Codice, si restringe la possibilità per l'interessato di opporsi a determinazioni di carattere contrattuale assunte nei suoi riguardi<sup>63</sup>. In altri termini, egli può opporsi al trattamento dei suoi dati e alla profilazione nel momento in cui riceve l'informativa. Ma se ciò non avvenisse, egli non potrà opporsi alle decisioni che il titolare del trattamento avrà adottato sulla base della profilazione già preventivamente autorizzata. La disposizione dell'art. 14, in realtà, è criticabile sotto due punti di vista. Innanzitutto, attraverso i rapporti contrattuali si soddisfano esigenze non necessariamente economiche della persona. La realizzazione dell'individuo nella società moderna, infatti, si manifesta anche nell'accesso a beni e servizi ai quali si accede contrattualmente. Pensiamo all'accesso al credito, all'istruzione o alla sanità privata, ai mezzi di comunicazione. In secondo luogo, poi, la norma dell'art. 14 disciplina la possibilità che uno dei due contraenti possa decidere in merito al rapporto contrattuale sulla base di profili automatizzati senza considerare le possibili posizioni di disparità fra i soggetti del contratto. Soprattutto nei rapporti contrattuali di consumo, si registrano frequentemente situazioni di vera disuguaglianza, anche solo informativa<sup>64</sup>.

Si può ritenere, allora, che una migliore tutela dell'autodeterminazione dell'interessato circa la profilazione dei suoi dati si debba tradurre nel ga-

<sup>62</sup> S. RODOTÀ, *Il diritto di avere diritti*, cit., 400.

<sup>63</sup> E. PELLECCIA, *Art. 17 (Limiti all'utilizzabilità di dati personali)*, cit., 472-473, secondo cui «all'ampliamento dell'area del divieto corrisponderebbe una proporzionale riduzione di quella nella quale una 'decisione automatizzata' sarebbe possibile e che finirebbe con il coincidere con quella nella quale il 'diritto di opposizione' è escluso».

<sup>64</sup> Sul punto, vedi le osservazioni

critiche di L. BOZZI, *Le regole generali per il trattamento dei dati*, cit., 101, secondo la quale «l'ammissibilità di decisioni "contrattuali" fondate unicamente su profili automatizzati e l'impossibilità di opporsi a tali decisioni indubbiamente possono condurre a situazioni in grado di compromettere e mortificare la dignità della persona, specie se si considera che il contratto può essere uno strumento per il soddisfacimento di interessi non solo economici».

rantire un sistema di *opt-in*, in base al quale la liceità del trattamento possa derivare esclusivamente dall'accettazione dell'interessato. Se si ritenesse, invece, che l'autodeterminazione possa essere individuata nella passività dell'interessato rispetto all'esercizio di una facoltà di *opt-out*, si sottovaluterebbe pericolosamente il fatto che l'attuale società dei consumi e dell'elettronica sottopone continuamente gli individui alla possibilità di lasciare tracce e informazioni sino al punto di perderne il controllo<sup>65</sup>.

In questo senso si può segnalare come proprio la regola dell'*opt-in* sia stata selezionata nella direttiva 2009/136/CE per regolare la profilazione delle informazioni rilasciate attraverso i *cookies* della navigazione su internet, spesso utilizzati dai *providers* come strumenti, più o meno occultamente installati sul *browser*, per parametrare l'offerta pubblicitaria ai gusti del singolo consumatore. In questi casi, infatti, si crea una maggiore necessità di controllo rispetto alla raccolta occulta o, quantomeno, inconsapevole di informazioni sugli utenti desumibili dalle loro sessioni di navigazione<sup>66</sup>. La direttiva è stata recepita nel nostro Paese con il decreto legislativo del 28 maggio 2012, n. 69, che impone la segnalazione all'utente della presenza di *cookies* e perciò, della possibilità che siano registrate le informazioni sulla navigazione effettuata dall'utente. All'utente deve essere garantita la scelta se accettare (attraverso l'*opt-in*) o rifiutare la registrazione.

Ma, probabilmente, la profilazione dovrebbe essere subordinata al consenso dell'interessato sempre, riconoscendo in ogni caso la necessità che la liceità del trattamento derivi dalla incontrovertibile accettazione dell'interessato ad essere profilato, nella piena consapevolezza delle finalità alle quali essa è rivolta.

#### ABSTRACT

*This research is proposed to critically examine the behavior of the law for an electronic practice of personal data processing, quite a lot invasive and dangerous for its potentiality to compromise the fundamental freedoms. After having verified how low is the interest of the law for the data profiling, the Author analyzes some of the main decisions of the Italian Data Protection Authority. It results the need of implementing a legal regulation for the profiling based on the general principles of transparency, freedom of consent and proportionality in the personal data processing. On this subject, moreover, it is particularly important to supervise that the consent will always correspond to a full self-determination of the profiled persons and to a complete awareness of the finalities underlying to the data processing.*

<sup>65</sup> Sul punto, molto efficaci le considerazioni di A. MANTELER●, *Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies*, cit., 791-793, in merito al fatto che l'indifferenza o l'inconsapevolezza dell'internauta può portare ad una indiscri-

minata accettazione di cookies nella quale non si può ravvisare « una valida manifestazione di volontà, venendo a mancare la specificità del consenso manifestato ».

<sup>66</sup> Vedi le disposizioni introdotte con la direttiva 2009/136/CE, in G.U.C.E., 18 dicembre 2009, L 337/11.