# 8 I trattamenti da parte di Forze di polizia e per finalità di *intelligence*

## 8.1. *Il controllo sul Ced del Dipartimento della pubblica sicurezza*

A seguito di segnalazioni ricevute, l'Autorità ha continuato ad assicurare il riscontro da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno e di uffici periferici della Polizia di Stato alle richieste degli interessati sia di accesso e comunicazione dei dati conservati presso il Centro elaborazione dati (Ced), sia di eventuale rettifica dei dati medesimi, nel rispetto delle disposizioni poste dall'art. 10, l. 1° aprile 1981, n. 121, come modificato dall'art. 175 del Codice.

## 8.2. *Gli altri interventi in relazione alle Forze di polizia*

**Affissione e trasmissione dal Ministero della giustizia alle OO.SS. dell'elenco nominativo degli agenti di polizia penitenziaria che effettuano lavoro straordinario**

Un agente del Corpo della polizia penitenziaria ha segnalato l'affissione mensile, in alcuni locali del Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia, dell'elenco del personale del Corpo nei confronti del quale era stata disposta la liquidazione del compenso per prestazioni di lavoro straordinario, con l'indicazione del numero di ore effettuate e di quelle retribuite o compensate con turni di riposo, nonché la trasmissione di tale elenco alle organizzazioni sindacali.

A tale proposito, richiamati i principi di necessità, non eccedenza, liceità e qualità dei dati (artt. 3 e 11 del Codice) nonché le disposizioni specifiche dettate per il trattamento dei dati da parte dei soggetti pubblici (nella specie, in particolare, gli artt. 18 e 19, comma 3 del Codice), il Garante ha osservato che le "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", adottate il 14 giugno 2007 (in G.U. 13 luglio 2007, n. 161, doc. web n. 1417809), prevedono, che non è di regola lecito per il datore di lavoro pubblico diffondere informazioni personali riferite a singoli lavoratori (punto 6.3) e che, in difetto di disposizioni del contratto collettivo applicabile che prevedano espressamente che l'informazione sindacale abbia ad oggetto anche dati nominativi del personale, l'amministrazione può fornire alle organizzazioni sindacali solo dati numerici o aggregati (punto 5).

Nella specie, il Garante, rilevata la mancanza di specifica fonte normativa o negoziale (non rinvenibile, in particolare, nell'art. 10, comma 9, dell'Accordo nazionale quadro per il personale appartenente al Corpo di polizia penitenziaria) che preveda che gli elenchi relativi al personale che effettua lavoro straordinario, oggetto di affissione e comunicazione alle organizzazioni sindacali, venga redatto con l'indicazione del nominativo dei lavoratori interessati, ha dichiarato illecito il relativo trattamento, vietandone la prosecuzione da parte del Dipartimento dell'amministrazione penitenziaria, che ha ottemperato (provv. 18 luglio 2013, n. 358, doc. web n. 2578201).

**Ostensione da parte degli ospedali alla polizia amministrativa della certificazione medica relativa a persone coinvolte in sinistri stradali**

Una Prefettura ha sottoposto un quesito relativo alla legittimità del diniego, da parte di un ospedale, all'ostensione agli organi di polizia amministrativa della certificazione medica relativa a persone coinvolte in sinistri stradali, ai fini della successiva trasmissione alla prefettura per la determinazione del periodo di sospensione della patente di guida del conducente responsabile del sinistro, *ex* artt. 222 e ss. del codice della strada. Ritenuto che la comunicazione tra pp.aa. di dati sensibili per finalità

amministrative è ammessa dal Codice unicamente quando è prevista da una norma di legge o di regolamento (art. 19, comma 3), l'Ufficio ha chiarito che il trattamento in oggetto può essere legittimamente effettuato dalle Aziende sanitarie solo ove sia previsto nel relativo regolamento adottato in conformità allo schema tipo sul quale il Garante ha espresso parere favorevole con provvedimento del 26 luglio 2012, n. 220 (doc. web n. 1915390). Laddove si renda, tuttavia, indispensabile trattare ulteriori categorie di dati, o eseguire altre operazioni di trattamento per perseguire finalità di rilevante interesse pubblico individuate dalla legge, le integrazioni o modifiche devono essere sottoposte al parere del Garante (nota 12 aprile 2013).

**Conferenze stampa nel corso di indagini giudiziarie**

Un avvocato, in qualità di difensore d'ufficio di una persona indagata in un procedimento penale, ha lamentato una violazione della disciplina in materia di protezione dei dati personali da parte di funzionari di polizia che nel corso di una conferenza stampa avevano divulgato, oltre alla forografia e alle generalità del suo assistito, anche presunte frasi a lui attribuite e particolari del crimine che avrebbero potuto rilevarsi, per la natura del reato e il coinvolgimento dei familiari della persona offesa, pericolosi per l'incolumità dell'indagato e forieri di problemi di ordine pubblico.

L'Ufficio ha evidenziato che, come emerso nel corso dell'istruttoria, obiettivo della conferenza stampa era accertare se l'interessato si fosse reso protagonista di episodi simili ai danni di altre persone. La diffusione delle informazioni a livello locale e la loro conoscenza da parte della collettività avrebbe potuto rivelarsi utile, se non necessaria, per verificare se altre persone avessero subito i medesimi abusi. In tale situazione, pur considerando le ragioni di riservatezza e di presunta incolumità dell'interessato, doveva ritenersi lecita, ai sensi degli artt. 11 e 47 del Codice, la divulgazione – peraltro autorizzata dalla Procura della Repubblica competente – dei dati dell'indagato e delle circostanze della vicenda, tenuto conto delle esigenze di giustizia sottese alla diffusione delle informazioni (nota 25 gennaio 2013).

**Accertamenti di polizia giudiziaria**

Sono stati chiesti chiarimenti da parte di un medico, amministratore unico e legale rappresentante di uno studio medico, riguardo alle informazioni che, senza ledere la riservatezza dei pazienti, è possibile comunicare su richiesta della polizia giudiziaria (nella specie, se una determinata persona si fosse recata presso il suo studio medico, quali esami avesse svolto e se in regime di convenzione o mediante pagamento da parte dell'assistito).

Al riguardo l'Ufficio ha evidenziato che, ai sensi dell'art. 256 c.p.p., i medici – al pari degli altri soggetti indicati negli artt. 200 e 201 c.p.p. – devono consegnare all'autorità giudiziaria che ne faccia richiesta, tra l'altro, gli atti, i documenti e le informazioni di cui siano in possesso per ragioni della loro professione, salvo che dichiarino per iscritto che si tratta di segreto inerente alla loro professione. Peraltro, l'autorità giudiziaria che ritiene di non potere procedere senza acquisire gli atti può provvedere alla verifica di tale dichiarazione e, se risulta infondata, può disporne il sequestro. Risulta quindi necessario che il medico verifichi se i dati oggetto della richiesta della polizia giudiziaria rientrino tra quelli coperti dal segreto professionale, attenendosi, in tal caso, a quanto prevede l'art. 256 c.p.p. (nota 16 aprile 2013).

**Accesso delle OO.SS. negli istituti penitenziari**

L'Autorità ha fornito riscontro a un quesito del Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia concernente la possibilità da parte delle organizzazioni sindacali di effettuare riprese foto-video nel corso delle visite sui luoghi di lavoro degli istituti penitenziari previste dall'art. 5, comma 6, dell'Accordo nazionale quadro del 24 marzo 2004, il quale afferma che la visita dei rappresentanti sindacali "è diretta a verificare esclusivamente le condizioni logistiche dei vari luoghi di lavoro".

L'Ufficio ha rilevato che la disposizione risulta fare chiaro riferimento alla verifica dei luoghi frequentati dagli agenti della polizia penitenziaria nello svolgimento della loro attività lavorativa – quali uffici, spazi dedicati alla custodia dei detenuti, locali

vari, eventuali apparecchiature utilizzate, postazioni di lavoro, *etc.* – in funzione della loro idoneità a consentire l'espletamento dei compiti di istituto in condizioni di salubrità e sicurezza. In tale contesto, le ipotizzare riprese foto-video vanno limitate alle sole condizioni degli ambienti, con esclusione di profili attinenti alla protezione dei dati personali. L'eventuale coinvolgimento nelle riprese del personale operante negli istituti, come pure dei detenuti ivi ristretti, in quanto non essenziale rispetto al fine del controllo dei luoghi di lavoro demandato alle organizzazioni sindacali dal contratto collettivo, comporterebbe, infatti, un trattamento di dati effettuato in violazione del principio di necessità ed eccedente rispetto alle finalità perseguite con le verifiche previste dalla contrattazione (cfr. artt. 3 e 11, comma 1, lett. *d*), del Codice) (nota 10 maggio 2013).

*8.2.1. I sistemi di videosorveglianza per finalità di pubblica sicurezza*

**Visione degli interni di private abitazioni da parte di telecamere installate per motivi di pubblica sicurezza**

L'Autorità ha ricevuto la segnalazione di alcuni cittadini, residenti in diversi comuni, circa la presenza di telecamere di videosorveglianza che, pur installate sulla pubblica via, consentivano, a causa della loro ubicazione, una visione diretta anche degli interni delle abitazioni dei segnalanti. Gli accertamenti effettuati dall'Autorità hanno permesso di appurare che le telecamere erano state installate in attuazione del "Programma Operativo Nazionale (PON) – Sicurezza per lo Sviluppo – Obiettivo convergenza 2007-2013", gestito dal Ministero dell'interno, e che la titolarità del trattamento dei dati era stata conferita alla locale questura. Il Garante ha ritenuto che, ancorché gli obiettivi del menzionato programma – riconducibili alla prevenzione e al contrasto alla criminalità – apparissero condivisibili e di notevole rilevanza sociale, i trattamenti di dati personali effettuati tramite l'utilizzo di sistemi di videosorveglianza, quand'anche riconducibili a quelli previsti dall'art. 53 del Codice, debbono rispettare i principi posti dall'art. 11 del Codice medesimo e, in particolare, il principio secondo il quale i dati personali oggetto di trattamento debbono essere pertinenti e non eccedenti rispetto alle finalità per le quali i dati sono raccolti o successivamente trattati, come ribadito dal Garante anche nel provvedimento generale in materia di videosorveglianza adottato l'8 aprile 2010 (doc. web n. 1712680). La possibilità per le telecamere in argomento di effettuare riprese anche all'interno degli immobili dei segnalanti configura quindi un trattamento di dati personali illecito in quanto eccedente e non pertinente rispetto alle finalità di prevenzione e contrasto alla criminalità per le quali i dati sono raccolti. Pertanto, il Garante ha vietato alla questura il trattamento dei dati personali dei segnalanti attraverso le citate telecamere di sorveglianza, prescrivendo, altresì, di adottare ogni misura necessaria atta a impedire la possibilità di effettuate riprese dell'interno delle abitazioni dei medesimi, dandone riscontro al Garante. Il titolare del trattamento ha provveduto ad apportare al sistema di videosorveglianza le modifiche richieste (provv.ti 27 giugno 2013, n. 316, doc. web n. 2576958 e n. 317, doc. web n. 2577003).

**Tempi di conservazione delle immagini riprese dai sistemi di videosorveglianza della polizia municipale**

Il Corpo della polizia municipale di un Comune ha chiesto se, per corrispondere alle eventuali esigenze investigative delle Forze di polizia, era possibile prolungare fino ad un periodo di 60 giorni i tempi di conservazione delle immagini delle targhe di veicoli registrate dal sistema di videosorveglianza gestito dal Corpo medesimo. L'Ufficio ha rilevato che il paragrafo 3.4. del provvedimento generale in materia di videosorveglianza, prevede che i comuni, in caso di videosorveglianza finalizzata alla tutela della sicurezza urbana, possono conservare i dati nel termine massimo di sette giorni successivi alla rilevazione delle immagini e che, in caso di effettive ed eccezionali esigenze di ulteriore conservazione, devono inoltrare al Garante una richiesta di verifica preliminare, adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti

eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità.

Con riferimento al caso di specie, il provvedimento consente quindi un prolungamento del termine di conservazione delle immagini anche in presenza di richieste della polizia giudiziaria motivate però in relazione a specifiche e puntuali attività investigative in corso, dovendosi escludere una preventiva e generalizzata conservazione ultrasettimanale per esigenze solo eventuali (nota 9 dicembre 2013).

**Videosorveglianza all'interno delle camere di sicurezza**

Un Comune ha posto un quesito relativo alla liceità del trattamento dei dati personali svolto per mezzo dell'installazione di telecamere che riprendano l'interno delle camere di sicurezza del comando della polizia municipale ove, ai sensi degli artt. 380 o 381 c.p.p., vengono rinchiusi gli arrestati in flagranza di reato da personale con qualifica di agente od ufficiale di polizia giudiziaria. Il Comune ha evidenziato che le immagini sarebbero state visionate dal personale del comando e conservate per un massimo di 24 ore, consentendo di poter controllare a distanza i detenuti al fine di intervenire in caso di tentativo di evasione e per evitare possibili atti di autolesionismo.

Fornendo riscontro, l'Aurorità ha rappresentato che la circostanza che le camere di sicurezza debbano essere sottoposte a sorveglianza non implica per ciò solo che sia previsra e consentita l'installazione di telecamere che riprendano l'interno delle stesse. Rilevato che non risulta sussistere – né è stata indicata dal comando – alcuna specifica normativa concernente la videosorveglianza nelle camere di sicurezza, è stato evidenziato che la Corte di cassazione, nel pronunciarsi su una vicenda relativa ad un detenuto sottoposto al regime di cui all'art. 41-*bis*, l. n. 354/1975, ha ritenuto illegittimo il ricorso alla videosorveglianza totale dello stesso – anche nel momento dell'utilizzo della *toilette* –, valutando idonei a prevenire possibili aggressioni alla persona del detenuto i controlli fisici diretti mediante feritoie ed oblò (Cass. pen., sez. V, 26 aprile 2011). Occorre dunque assumere come riferimento la normativa generale in materia di protezione dei dati posta dal Codice e, più specificamente, i principi posti dall'art. 11, oltre alle prescrizioni contenute nel provvedimento generale del Garante in materia di videosorveglianza.

In particolare, nella materia rilevano i principi di necessità e di proporzionalità nel trattamento dei dati, rispetto ai quali occorre valutare, ad esempio, se sia necessario installare le telecamere all'interno delle camere di sicurezza o se sia sufficiente posizionarle negli ambienti attigui alle celle, oppure ancora se corrisponda alle esigenze esposte dal comando dotare di telecamere solo una o più celle, da utilizzare nei soli casi, da valutare rigorosamente volta per volta, in cui sussistano effettive e concrete esigenze di prevenire possibilità di evasione o pericoli alla persona, rimanendo sempre ferma, come ha chiarito la citata pronuncia della Suprema Corte, la salvaguardia degli aspetti più intimi della sfera di riservatezza dell'interessato. Le conseguenti valutazioni non possono comunque essere assunte con carattere di generalità, ma devono essere svolte caso per caso e, ove ritenuto necessario il trattamento in esame, devono essere supportate da una circostanziata motivazione (nota 5 settembre 2013).

### 8.3. *Il controllo sul sistema di informazione Schengen*

Il Ministero dell'interno-Dipartimento della pubblica sicurezza ha rappresentato l'opportunità di differire l'adempimento delle ultime misure prescritte dal Garante volte a rafforzare la sicurezza nel trattamento dei dati effettuati per l'attuazione della Convenzione di Schengen, in ragione sia delle innovazioni tecnologiche introdotte con l'entrata in funzione del nuovo Sistema di informazione Schengen (SIS II), sia

delle difficoltà di realizzazione dei progetti, legate soprattutto alla disponibilità delle necessarie risorse finanziarie.

Alla luce delle indicazioni ricevute e delle difficoltà rappresentate dal Ministero, il Garante con provvedimenti del 24 gennaio 2013, n. 23 (doc. web n. 2324763) e 1° agosto 2013, n. 379 (doc. web n. 2635313) ha disposto il differimento dei termini per l'adempimento delle prescrizioni, che sono in corso di attuazione.

**Accesso diretto**

Il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nell'N-SIS, in virtù delle quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale del SIS, ossia al Dipartimento della pubblica sicurezza (cd. accesso diretto). Il numero e il contenuto delle richieste degli interessati che ancora pervengono direttamente al Garante sono rimaste stabili rispetto all'anno precedente.

Hanno invece subito un lieve aumento le richieste di accesso ai dati pervenute al Garante da Autorità di controllo di sezioni nazionali del SIS di altri Stati, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane. Le informazioni sono state comunicate, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni degli artt. 109 e 114 della Convenzione.

### 8.4. *Il* Datagate *e i trattamenti per finalità di* intelligence

A fronte delle notizie, riportate dalla stampa, sul cd. *Datagate* – ovvero sulla raccolta di dati personali di milioni di cittadini, non solo statunitensi, da parte della *National Security Agency* (NSA) – il Garante ha svolto una serie di attività informative e di impulso nei confronti del Governo, al fine di minimizzare i rischi per i cittadini italiani rispetto ad eventuali acquisizioni dei loro dati per fini di *intelligence*.

In primo luogo, il 23 luglio 2013 il Garante è stato audito, ai sensi dell'art. 31, comma 3, l. n. 124/2007, dal Comitato parlamentare per la sicurezza della Repubblica (Copasir), in relazione alle implicazioni sui diritti dei cittadini europei alla raccolta di dati personali per fini di *intelligence* svolta in base al *Foreign Intelligence Surveillance Act* (FISA) e al rapporto tra protezione dati e trattamenti per fini di sicurezza dello Stato nel nostro ordinamento.

Il 22 ottobre, all'indomani dell'approvazione in Commissione LIBE del Parlamento europeo, della proposta di regolamento sulla protezione dei dati personali, il Garante, con una nota indirizzata al Presidente del Consiglio dei Ministri, ha segnalato l'esigenza di accertare se lo spionaggio anche telematico condotto dal NSA abbia coinvolto, sia pure incidentalmente, cittadini italiani, nonché la necessità di adottare efficaci strumenti di protezione dei dati personali trattati per fini di sicurezza, anche nella consapevolezza e condivisione dell'obiettivo europeo di rafforzare gli strumenti di cooperazione di polizia e giudiziaria (doc. web n. 2708275).

Infine, l'11 novembre 2013 il Garante e il Dipartimento delle informazioni per la sicurezza (Dis) della Presidenza del Consiglio dei Ministri hanno siglato un protocollo d'intenti volto a disciplinare alcune procedure informative funzionali all'esercizio delle rispettive attribuzioni. Il protocollo prevede, in particolare, modalità di informazione idonee a consentire al Garante di conoscere alcuni elementi essenziali del trattamento dei dati personali effettuato dagli Organismi per l'informazione e la sicurezza in alcuni contesti peculiari, segnatamente quelli concernenti la sicurezza cibernetica o gli accessi alle banche dati delle pp.aa. o degli esercenti servizi di pubblica utilità.

# 9 L'attività giornalistica

Tenendo conto delle diverse forme attraverso cui si esercita ormai la libertà di informazione, l'anno di riferimento è stato caratterizzato da un impegno costante nel valutare, nel quadro di riferimento del Codice (in particolare, artt. 136-139) e dell'allegato codice di deontologia, segnalazioni e reclami per lo più concernenti l'esercizio dell'attività giornalistica.

Accanto a tale attività, improntata al bilanciamento tra libertà di informazione e diritto alla riservatezza e alla protezione dei dati personali, è maturata la decisione di promuovere l'aggiornamento del codice di deontologia, adottato nel 1998, relativo al trattamento di dati personali in ambito giornalistico al fine di un suo adeguamento in considerazione dell'evoluzione tecnologica (che ha inciso su tecniche e modalità dell'informazione) e dell'evoluzione giurisprudenziale di alcuni istituti, quali il "diritto all'oblio" (cui peraltro fa riferimento la proposta di regolamento Ue in materia di protezione di dari personali).

Il Garante ha quindi deliberato l'avvio dei lavori, secondo la procedura di cooperazione con il Consiglio nazionale dell'Ordine dei giornalisti prevista dall'art. 139 del Codice, contemplando altresì la possibilirà di sentire, in rale ambito, anche soggetri rappresentativi dell'informazione *online* (provv. 1° agosto 2013, n. 376, in G.U. 23 agosto 2013, n. 197, doc. web n. 2564822). La presidenza dell'Ordine dei giornalisti e il Garante, renuto anche conto dei contributi pervenuti e degli elementi acquisiti dai soggetti interpellati, hanno lavorato ad una bozza di nuovo codice di deontologia da sottoporre al Consiglio dell'Ordine dei giornalisti nella riunione plenaria del 27-30 marzo 2014, nel corso della quale, tuttavia, il testo non è stato approvato.

Il Garante, nell'esprimere alla presidenza dell'Ordine il proprio rammarico per la valutazione negativa espressa dal Consiglio rispetto ad un lavoro attento e approfondito svolto anche con il proprio contributo, ha comunicato all'Ordine di non essere intenzionato ad esercitare i poteri sosritutivi offerti dall'art. 139 del Codice ai fini dell'approvazione del testo e di voler proseguire nei propri compiti attenendosi al codice di deontologia vigente.

## 9.1. *I minori*

Il delicato rapporto tra informazione e turela dei minori (nel quadro delle fonti sopra ricordate nonché della Carta di Treviso) conserva una posizione centrale nello svolgimento dei compiti istituzionali dell'Autorità. Nella vigente cornice normativa, come noto, il diritto del minore alla riservatezza deve sempre essere considerato prevalente rispetto al diritto di cronaca e, al fine di tutelarne la personalità, i giornalisti devono rendere non identificabili i minori coinvolti in fatti di cronaca (art. 7 codice di deontologia).

L'Autorità ha invocato tali principi nell'esaminare, in particolare, due casi, sottoposti alla sua attenzione da due Tribunali per i Minorenni, riguardanti delicate vicende familiari di affidamento. Nel primo caso una testata giornalistica locale aveva pubblicato la notizia del suicidio di una donna, madre di tre figli affidati a terzi (in ragione del problemarico contesto familiare in cui si trovavano) con un provvedimento giuri-

sdizionale; oltre alla foto e alle generalità della donna, il giornale aveva pubblicato quelle dei nonni e i nomi dei minori (questi ultimi contenuti nelle pagine del diario personale della madre, pure pubblicate dal quotidiano), rendendoli così direttamente identificabili (nota 22 febbraio 2013).

Nella seconda vicenda, un giornale locale aveva pubblicato il nome e il cognome di un minore, allontanato dai genitori con un provvedimento giurisdizionale, unitamente ad altre informazioni che ne evidenziavano la situazione di disagio e una possibile patologia; nell'articolo venivano altresì pubblicati i dati identificativi dell'intero nucleo familiare, compresi quelli dei fratelli, anch'essi minori (nota 13 settembre 2013).

L'Ufficio, nel ritenere entrambe le pubblicazioni contrastanti con la disciplina di protezione dei dati personali (oltre che con la Carta di Treviso che tutela espressamente "l'anonimato del minore per non incidere sull'armonico sviluppo della sua personalità"), ha ribadito che le garanzie a favore dei minori operano anche nell'eventualità che siano i genitori a rilasciare dichiarazioni alla stampa.

Analoghe valutazioni critiche sono state formulate in relazione alla perdurante diffusione, anche in rete, di notizie e immagini relative al bambino di Padova prelevato a scuola dalle Forze dell'ordine in esecuzione di un provvedimento giurisdizionale di affidamento, caso di cui l'Autorità si era già occupata (cfr. Relazione 2012, p. 148). Ulteriori segnalazioni concernenti la medesima vicenda hanno evidenziato che taluni organi di informazione, nel riferire dello svolgimento di un procedimento giudiziario coinvolgente i genitori, non solo hanno nuovamente fatto riferimento al minore – talvolta identificato nominativamente o, indirettamente, tramite i nominativi dei familiari – ma hanno anche riportato dichiarazioni rese dal padre nel corso del giudizio concernenti delicati episodi della vita privata del figlio. L'Ufficio ha considerato tale pubblicazione un'ulteriore significativa intrusione nella sfera privata del minore in violazione delle speciali garanzie dettate dall'ordinamento ed ha pertanto invitato gli editori interessati – che hanno formalmente aderito a tale richiesta – ad impegnarsi autonomamente a non diffondere ulteriormente, anche nelle edizioni *online* dei rispettivi giornali, dettagli relativi alla vita privata del minore (nota 5 dicembre 2013).

L'Autorità ha poi richiamato pubblicamente gli organi di informazione al rispetto del codice di deontologia e della Carta di Treviso in relazione alla diffusione di notizie concernenti fatti di cronaca di particolare risonanza avvenuti a Roma (una vicenda di prostituzione minorile e un tentativo di suicidio da parte di un sedicenne) rispetto ai quali sono stati via via diffusi – attraverso i *media* tradizionali e in rete – dettagli non essenziali lesivi della personalità e della dignità dei minori interessati, aumentando il rischio di una loro identificazione (comunicati stampa 29 maggio e 13 novembre 2013, docc. web nn. 2449404 e 2749736).

### 9.2. *La cronaca giudiziaria*

**Notizie e immagini di arrestati e indagati**

La materia della diffusione di informazioni relative a vicende giudiziarie ha continuato a formare oggetto di attenzione da parte dell'Autorità che ha ritenuto prive di fondamento segnalazioni nelle quali si lamentava la diffusione di dati identificativi di persone sottoposte ad indagine o condannate alla luce del principio, più volte ribadito nei suoi provvedimenti, secondo cui la pubblicazione di dati personali relativi a procedimenti penali è ammessa, anche senza il consenso dell'interessato, nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice; artt. 6 e 12 del codice di deontologia) (*ex pluribus*, note 15 marzo, 17 maggio e 21 ottobre 2013).

**Pubblicazione di atti del procedimento e intercettazioni**

Segnalazioni e reclami concernenti la cronaca giudiziaria talora hanno evidenziato profili di illiceità rispetto non solo al Codice, ma anche alle disposizioni in materia di segreto delle indagini e di pubblicazione degli atti processuali (artt. 114 e 329 c.p.p. e art. 684 c.p.).

In una vicenda, concernente la pubblicazione su un sito internet di un *e-book* recante il testo delle intercettazioni telefoniche raccolte nell'ambito di un'indagine coordinata dalla Procura della Repubblica di Napoli e contenute in un'informativa preliminare predisposta dai Carabinieri, anche alla luce del riscontro pervenuto dalla menzionata Procura, l'Autorità ha ritenuto che la pubblicazione, per le sue caratteristiche (il contenuto del libro coincideva con l'intero atto-informativa dei Carabinieri, comprensivo di intestazione, non sottoposto a rielaborazione alcuna), potesse presentare elementi di incompatibilità con l'art. 114, comma 2, c.p.p. – che vieta "la pubblicazione, anche parziale, degli atti non più coperti dal segreto fino a che non siano concluse le indagini preliminari ovvero fino al termine dell'udienza preliminare" –, sottoponendo quindi l'accertamento di tale circostanza alla competente autorità giudiziaria.

Si è d'altra parte evidenziato che, sotto il profilo delle specifiche disposizioni vigenti in materia di trattamento di dati personali in ambito giornalistico (artt. 136-139 del Codice), la pubblicazione, pur se attinente a fatti di indiscutibile interesse pubblico (risultanze di indagini su ipotesi di reato connessi alla gestione dei contributi pubblici erogati a favore di un movimento politico), contenesse alcune espressioni lesive della dignità della reclamante (senatrice, esponente del movimento interessato dalle indagini, menzionata nelle conversazioni intercettate), non rispondenti al parametro dell'"essenzialità dell'informazione", risultando la stessa di fatto estranea alla vicenda della gestione dei fondi pubblici attribuiti al movimento politico (nota 14 giugno 2013).

**Vittime di reato**

Particolare cautela nella diffusione di notizie relative a procedimenti penali deve essere adoperata a protezione del diritto alla riservatezza nonché per assicurare il rispetto della dignità delle persone offese dal reato, poiché la pubblicità (specie tramite internet) data alla lesione ne pregiudica ulteriormente i diritti. Questo orientamento è stato alla base della valutazione di illiceità della pubblicazione in rete, da parte di una testata locale, di due articoli (successivamente rimossi) nei quali erano stati riportati brani di un libro, incentrato sulla reclamante (peraltro con riferimenti lesivi della sua dignità) e sulla sua famiglia, dichiarato giudizialmente diffamatorio e oggetto di sequestro (nota 28 ottobre 2013).

### 9.3. *I personaggi pubblici*

Per quanto riguarda la diffusione di informazioni riguardanti personaggi pubblici o che esercitano pubbliche funzioni il quadro normativo e la relativa evoluzione giurisprudenziale consentono invece di individuare margini più ampi nel trattamento dei dati personali (in tal senso v. già Relazione 2012, p. 153).

Tale orientamento è stato seguito anche in relazione alla lamentata diffusione, nel corso di una trasmissione televisiva di inchiesta e di approfondimento informativo, di immagini tratte da un Dvd della festa nuziale privata dei segnalanti asseritamente sottratto agli stessi. Al riguardo, l'Ufficio ha rilevato che – fermi restando gli accertamenti dell'autorità giudiziaria in ordine all'asserita acquisizione fraudolenta del Dvd – la diffusione delle immagini ritraenti i segnalanti e alcuni ospiti (e tra questi un esponente politico già ministro dello sviluppo economico) non presentava profili di contrasto con il parametro della "essenzialità dell'informazione riguardo a fatti di interesse pubblico" (art. 137, comma 3, del Codice). Il servizio andato in onda – nel quale, peraltro, i volti degli altri ospiti presenti alla festa erano stati oscurati – si inseriva, infatti,

nell'ambito di un dibattito sui criteri in base ai quali vengono corrisposti contributi e altre utilità pubbliche a privati e aveva lo scopo di documentare l'esistenza di frequentazioni, anche di natura non professionale, tra l'esponente politico ritratto e i segnalanti (l'uno, presidente della Associazione italiana per lo sviluppo e la promozione del digitale terrestre, l'altra, amministratrice di un consorzio assegnatario di un'autorizzazione pubblica per l'utilizzo del digitale terrestre) (nota 28 marzo 2013).

Il Garante ha invece ritenuto travalicati i limiti della libertà di espressione in relazione alla diffusione in rete del contenuto di *e-mail* private, presumibilmente copiate da *hacker*, di alcuni parlamentari. L'Autorità ha rilevato come tale condotta potesse determinare una violazione della libertà e segretezza della corrispondenza (art. 15 Cost.) e delle specifiche garanzie poste a tutela delle comunicazioni e della corrispondenza dei membri del Parlamento (art. 68 Cost.) nonché la configurabilità del reato di cui all'art. 616 c.p. È stata altresì evidenziata una lesione del diritto alla riservatezza e alla protezione dei dati personali non solo dei parlamentari intestatari degli indirizzi di posta elettronica, ma di tutti coloro che sono entrati in contatto con essi attraverso la posta elettronica nonché dei terzi citati all'interno delle comunicazioni.

Il Garante, avendo individuato nella fattispecie un trattamento illecito ritenuto essere avvenuto *ab origine* in violazione di legge (art. 11, comma 1, lett. *a*) e *b*), del Codice) ed avendo rilevato che tale illiceità estendeva i suoi effetti anche ai successivi trattamenti (art. 11, comma 2, del Codice), ha vietato ogni ulteriore utilizzo delle *e-mail* in questione, prescrivendone la cancellazione (provv. 6 maggio 2013, n. 229, doc. web n. 2411368).

### 9.4. *L'uso di immagini in ambito giornalistico*

Su richiesta dell'Ufficio, talune testate *online* hanno rimosso i video con i quali, in un caso, si documentava la tragica morte di due operai impegnati nella manutenzione di una chiusa e, nell'altro si ritraeva il corpo senza vita di un uomo suicida (di cui erano state rese note generalità e informazioni relative allo stato di salute). In entrambi i casi l'Ufficio ha motivato la richiesta ritenendo non giustificata la diffusione delle immagini sul piano dell'essenzialità dell'informazione a fronte della legittima aspettativa di riserbo e di rispetto del dolore da parte dei familiari delle persone decedute (note 11 e 31 ottobre 2013).

**Tutela dei dati idonei a rivelare lo stato di salute**

L'Ufficio ha altresì ritenuto fondata la segnalazione di una donna (affetta da una grave patologia) in relazione ad un articolo che, nel documentare la decisione del giudice che aveva riconosciuto sussistente nel caso che riguardava la stessa un episodio di malasanità, aveva diffuso un insieme di dati (professione dell'interessata e la circostanza che fosse affetta da un'evidente menomazione fisica, professione del marito e composizione del nucleo familiare) i quali, nel loro complesso, consentivano di risalire all'identità della segnalante. L'Autorità ha precisato che, anche se l'identificabilità era avvenuta entro una cerchia ristretta di persone, queste ultime erano state comunque messe in condizione di conoscere informazioni sul suo stato di salute (che la segnalante aveva interesse a non rivelare). Nell'occasione è stato ribadito che il limite dell'"essenzialità dell'informazione" va interpretato con particolare rigore quando la notizia di cronaca investe fatti che incidono sulla salute di una persona "identificata o identificabile", richiamando anche la previsione del codice di deontologia secondo cui "il giornalista, nel far riferimento allo stato di salute di una determinata persona, identificata o identificabile, ne rispetta la dignità, il diritto alla riservatezza e al decoro personale, specie nei casi di malattie gravi o terminali, e si astiene dal pubblicare dati analitici di interesse strettamente clinico" (art. 10, comma 1) (nota 1° agosto 2013).

Analogamente è stata ritenuta fondata la doglianza di una donna che aveva lamentato una violazione della sua riservatezza da parte di un giornale locale che, nel riferire del decesso del fratello a causa di una grave malattia, aveva altresì rivelato (senza che ciò fosse pertinente) analoga seria patologia di cui la stessa era affetta (nota 12 marzo 2013).

### 9.5. *Gli archivi storici e le informazioni* online

Anche nel 2013 sono pervenute segnalazioni e ricorsi concernenti la reperibilità, a distanza di anni, tramite gli archivi storici *online* dei giornali, di dati personali a suo tempo pubblicati. Il Garante ha ribadito che la diffusione sul sito internet di un quotidiano *online* di un articolo contenente informazioni su fatti (anche molto delicati e risalenti) costituisce parte integrante dell'archivio storico della testata e non integra, in linea di principio, un illecito trattamento di dati personali. Tuttavia, tenuto conto del funzionamento della rete – che consente la diffusione di un gran numero di dati personali relativi a vicende anche remote – e in considerazione del tempo trascorso, ha ritenuto che una perenne associazione all'interessato della vicenda resa pubblica possa determinare un sacrificio sproporzionato dei suoi diritti. È stato quindi prescritto che la pagina web contenente i dati personali del ricorrente (anzitutto il suo nominativo) venisse deindicizzata, sottratta cioè alla diretta individuazione da parte dei comuni motori di ricerca, pur restando inalterata all'interno dell'archivio e consultabile telematicamente accedendo all'indirizzo web dell'editore (provv. 18 dicembre 2013, n. 594, doc. web n. 2957346) (cfr. par. 16.4).

In relazione ad un articolo contenente i dati identificativi dell'interessata (rimasta invalida a seguito di un intervento chirurgico) unitamente alla descrizione dettagliata delle relative patologie invalidanti, non rilevanti ai fini del diritto di cronaca, il Garante ha prescritto (con conseguente adempimento da parte dell'editore) la rimozione dell'articolo dagli archivi *online* (provv. 12 dicembre 2013, n. 578, doc. web n. 296950).

In altra fattispecie, vari siti internet e *blog*, dopo aver diffuso articoli relativi ad un collaboratore di giustizia, associando la nuova identità dallo stesso assunta quale effetto dell'adesione al programma di protezione a quella originaria, hanno provveduto ad eliminare tale associazione a seguito dell'intervento dell'Ufficio (nota 20 settembre 2013).

Si segnala, infine, il provvedimento adottato dal Garante il 21 novembre 2013, n. 516 (doc. web n. 2914227) ad esito di un ricorso, avente ad oggetto la richiesta di deindicizzazione dai motori di ricerca del testo di un'interrogazione parlamentare contenente dati giudiziari riferiti al ricorrente (molto risalenti nel tempo e superati da successivi sviluppi processuali) (cfr. par. 16.4).

### 9.6. *La persistente rintracciabilità sui motori di ricerca*

Ulteriori interventi dell'Autorità si sono resi necessari per assicurare il rispetto dei provvedimenti con cui era stato imposto il divieto di indicizzazione delle notizie contenute negli archivi *online*.

È stato più volte segnalato all'Autorità che, nonostante l'adozione di tutte le misure tecniche previste, alcuni contenuti, apparentemente non più indicizzabili, risultavano visualizzabili nell'indice di *Google search*. Nel novembre del 2013 l'Ufficio ha quindi chiesto, mediante contatti informali, chiarimenti a Google per meglio comprendere e individuare gli strumenti necessari per assicurare la definitiva deindicizzazione dei contenuti rinvenibili tramite il suo motore di ricerca e mira a definire tale aspetto nell'anno in corso, in modo tale da rendere possibilmente più chiara la *policy privacy* della società americana sul punto.

# 10 Il trattamento di dati personali attraverso internet e nel settore delle comunicazioni elettroniche

## 10.1. *L'utilizzo dei* cookie*: la consultazione pubblica e il tavolo di lavoro*

Nella Relazione 2012 sono state descritte le modifiche apportate alla disciplina relativa all'uso dei cd. *cookie* (i piccoli *file* di testo che i siti visitati dall'utente inviano al suo *browser* per essere poi ritrasmessi ai medesimi siti alla successiva visita del medesimo utente) e degli altri strumenti analoghi (*web beacon/web bug, clear* GIF, *etc.*) ad opera del d.lgs. 28 maggio 2012, n. 69, che ha novellato l'art. 122 del Codice in attuazione della direttiva 2009/136/CE.

Conclusasi la consultazione pubblica avviata dal Garante (con provv. 22 novembre 2012, n. 359, doc. web n. 2139697) al fine di individuare le modalità semplificate per l'informativa da rendere *online* sull'utilizzo dei *cookie* ai sensi dell'art. 13, comma 3, del Codice, l'analisi dei contributi pervenuti ha evidenziato non solo l'importanza dei menzionati dispositivi per la realizzazione della pubblicità *online* (tramite la profilazione degli utenti), ma anche per il funzionamento dei servizi offerti sulla rete. L'analisi delle problematiche emerse dalla consultazione ha indotto l'Autorità – in ragione della delicatezza della questione e dell'impatto della relativa disciplina sulla rete internet – ad avviare un tavolo di lavoro in materia (riunitosi per la prima volta il 18 settembre 2013) al quale sono stati invitati i partecipanti alla consultazione pubblica nonché esponenti del mondo accademico e della ricerca.

Gli ulteriori elementi acquisiti (anche all'esito di un incontro tenutosi presso l'Autorità nel febbraio 2014) sono attualmente al vaglio dell'Ufficio al fine di individuare le soluzioni giuridiche e tecniche idonee a garantire l'attuazione della normativa in materia.

## 10.2. *La conservazione dei dati di traffico* (data retention)

Nel 2013 si sono conclusi i procedimenti avviati a seguito del ciclo ispettivo effettuato dal Nucleo speciale *privacy* della Guardia di finanza in materia di conservazione di dati di traffico telefonico e telematico (di cui si è dato conto nella Relazione 2012, p. 259), volti alla verifica del rispetto delle prescrizioni impartite con il provvedimento generale del 17 gennaio 2008 (doc. web n. 1482111) integrato con successivo provvedimento generale del 24 luglio 2008 (doc. web n. 1538237), resosi necessario a seguito del recepimento della direttiva 2006/24/CE sulla conservazione dei dati di traffico mediante il d.lgs. 30 maggio 2008, n. 109 (che ha modificato, tra l'altro, l'art. 132 del Codice).

Rilevata, in sede di accertamento ispettivo, la mancata attuazione di alcune delle prescrizioni contenute nel menzionato provvedimento del luglio 2008, in considerazione delle criticità emerse le società hanno modificato le proprie procedure al fine di assicurare il rispetto della normativa in materia; in qualche caso, a seguito dell'adozione da parte del Collegio di provvedimenti prescrittivi, si sono adeguate nei termini previsti. In particolare, nei confronti di quattro società sono stati adottati provvedimenti prescrittivi per violazioni che hanno riguardato i tempi di conservazione

dei dati di traffico telefonico, superiori a quelli consentiti dalla legge – ed in relazione ai quali, a tacere di altri profili, si è incentrata la declaratoria di invalidità della Corte di giustizia dell'8 aprile 2014 (*Digital Rights Ireland* e *Seitlinger and Others*, Cause riunite C-293/12, C-594/12) – la mancata adozione di specifici sistemi di autenticazione informatica fondati su tecniche di *strong authentication*, di cui una necessariamente basata sull'elaborazione di caratteristiche biometriche dell'incaricato nonché la mancata adozione di alcune ulteriori misure di sicurezza. Tra queste, in particolare, la cifratura dei dati conservati, l'adozione di sistemi informatici disgiunti fisicamente per la conservazione dei dati per esclusive finalità di accertamento e repressione dei reati rispetto a quelli conservati per altre finalità, l'adozione di specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e della basi di dati (provv.ti 14 febbraio 2013, n. 64, doc. web n. 2313961; 21 febbraio 2013, n. 74, doc. web n. 2338534; 18 luglio 2013, n. 360, doc. web n. 2605222; 3 ottobre 2013, n. 429, doc. web n. 2740948).

In una delle fattispecie esaminate l'istruttoria è stata estesa dall'Ufficio con l'adozione di un ulteriore provvedimento prescrittivo relativo a violazioni della disciplina in materia di protezione dei dati personali concernenti il rilascio di un'informativa inidonea e le non corrette modalità di acquisizione del consenso (specifico e differenziato) da parte degli interessati (provv. 3 ottobre 2013, n. 430, doc. web n. 2745497).

All'attività ispettiva e ai conseguenti provvedimenti prescrittivi adottati dal Collegio ha fatto seguito l'avvio di numerosi procedimenti sanzionatori (cfr. par. 18.5).

### 10.3. *Le chiamate indesiderate effettuate per finalità promozionali* (*cd.* telemarketing *selvaggio*)

Alla modifica normativa che ha istituito il Registro pubblico delle opposizioni (d.P.R. n. 178/2010) ha corrisposto un incremento delle segnalazioni concernenti la ricezione di chiamate indesiderate sia nei confronti di utenze iscritte regolarmente al Registro (circa 2.300 segnalazioni), sia verso utenze a carattere riservato, in quanto non presenti negli elenchi, ivi comprese le utenze mobili.

Effettuate complesse attività istruttorie, anzitutto per determinare gli effettivi autori delle telefonate (essendo spesso oscurato il numero chiamante: *calling line identification*), si è potuto constatare che molti operatori economici si sono avvalsi, oltre che del proprio personale, anche di terzi i quali, a cascata, hanno ulteriormente demandato l'attività di contatto ad altri soggetti, talora stabiliti all'estero. Nell'insieme, l'esito dei suddetti accertamenti sul solo fenomeno delle chiamate indesiderate ha comportato in meno di tre anni (2011-2013) la contestazione di rilevanti sanzioni amministrative (cfr. par. 18.5).

Il fenomeno del *telemarketing*, con specifico riguardo alle sole segnalazioni relative al detto Registro (escludendo quindi, quelle relative a numerazioni non in elenco), ha fatto registrare una crescita esponenziale delle segnalazioni (circa 2.300 solo nell'anno 2013), larga parte delle quali è riferibile a più chiamate promozionali ascrivibili a prodotti e servizi commercializzati dalla medesima impresa. Al fine di offrire un'ampia tutela agli interessati e contrastare efficacemente il fenomeno (oggetto di ricorrente segnalazione), l'Autorità ha spesso avviato singole istruttorie preliminari (anche in mancanza dell'indicazione da parte del segnalante del numero chiamante).

### 10.4. *Le nuove regole per il contrasto alle cd. telefonate mute effettuate da* call center *con finalità di* marketing

Si è ampiamente riferito nella Relazione 2011 (p. 104 e ss.) delle telefonate cd. mute, ovvero effettuate mediante un sistema automatizzato per la generazione delle chiamate dirette agli abbonati telefonici che consente di mantenere in uno stato di attesa le chiamate che hanno già ricevuto risposta, suscettibili, quindi, di ingenerare allarme, ansia, sospetto e disturbo nei destinatari, fino al momento in cui un operatore di *call center* si rende disponibile.

In proposito merita segnalare che un primo provvedimento adottato dal Garante (provv. 6 dicembre 2011, n. 474, doc. web n. 1857326), oggetto di impugnazione, è stato integralmente confermato dal Tribunale di Roma (con sentenza n° 18977 depositata il 26 settembre 2013). In particolare, il giudice ha accolto la tesi del Garante stabilendo che "l'utilizzo dei dati personali per effettuare una chiamata muta in luogo che una proposta commerciale costituisce un trattamento di dati contrario al fondamentale canone della correttezza indicato dall'articolo 11 del Codice, atteso che tutto il sistema di selezione e formulazione delle chiamate [...] mira ad ottimizzare il successo delle chiamate passare agli operatori facendo ricadere il rischio e il disagio della chiamata muta sui destinatari".

Il fenomeno in esame ha peraltro fatto registrare un significativo incremento, specie negli ultimi mesi (alla fine del 2013, risultano pervenute circa 400 segnalazioni, alcune peraltro singolarmente riferibili a più episodi, anche ascrivibili a soggetti diversi), nonché la tendenza ad allarmanti picchi di chiamate mute effettuate da specifiche numerazioni in periodi di tempo determinati. Dalle verifiche e dagli approfondimenti conoscitivi effettuati, anche di carattere ispettivo, è emerso che in tutti i casi oggetto di segnalazione si trattava di telefonate effettuate da *call center* per finalità commerciali mediante l'impiego, ormai diffusissimo, di sistemi automatizzati di instradamento della chiamata agli operatori. Nella maggior parte dei casi le liste dei destinatari delle chiamate commerciali vengono "caricate" sulla piattaforma informatica utilizzata dai *call center* la quale, mediante l'impiego di un *software*, compone i numeri e smista le telefonate ai diversi operatori.

Con decisione n. 482 del 30 ottobre 2013 (doc. web n. 2740497) l'Autorità ha posto in consultazione pubblica per 60 giorni (dandone avviso sulla G.U. del 22 novembre 2013, n. 274) uno schema di provvedimento generale che individua una serie di misure per rendere il trattamento conforme alle disposizioni del Codice. In tale prospettiva, in particolare: 1) i *call center* dovranno censire correttamente e secondo criteri uniformi le chiamate mute effettuate agli interessati, la cui attesa non potrà prolungarsi oltre i 3 secondi, intervallo temporale oltre il quale la chiamata dovrà essere "abbattuta" dal sistema; 2) il numero di chiamate mute considerate entro la soglia di tollerabilità fisiologica non potrà essere superiore al 3% di tutte le chiamate andate a buon fine; tale percentuale dovrà essere misurata ad intervalli decadali e comunque nell'ambito di ogni singola campagna di *telemarketing*; 3) alla risposta dell'utente non potrà mai far riscontro il silenzio, che dovrà invece essere sostituito da un rumore sintetico ambientale (cd. *comfort noise*) con rumori di sottofondo, squilli di telefono, brusio, *etc.*, per dare la sensazione che la chiamata non provenga da molestatori; 4) a seguito di una chiamata muta, l'utente non potrà essere ricontattato prima di una settimana e comunque al contatto successivo dovrà essere prevista una modalità di instradamento automatico della chiamata stessa in modo da assicurare la presenza di un operatore; 5) i *call center* dovranno conservare per almeno due anni i *report* statistici della chiamate mute effettuate, in modo da consentire gli opportuni controlli.

### 10.5. *Il trattamento di dati personali effettuato mediante* call center *ubicati al di fuori dell'Unione europea*

Il trasferimento di molte attività verso *call center* insediati in Paesi non appartenenti all'Unione europea, nei quali potrebbero non essere assicurate le adeguate garanzie per i diritti degli interessati previste dalla normativa comunitaria, ha messo in luce possibili criticità sulle modalità di trattamento dei dati. Già a partire dal 2010, la questione della delocalizzazione all'estero delle attività di *call center* è stata riportata da diverse fonti di stampa e segnalata al Garante da strutture sindacali e associazioni di consumatori.

Successivamente, come noto, l'art. 24-*bis*, d.l. 22 giugno 2012, n. 83 convertito con modificazioni, dalla l. 7 agosto 2012, n. 134 (in G.U. 11 agosto 2012, n. 187), ha prescritto alle imprese che intendano spostare la propria attività al di fuori del territorio nazionale di darne previa comunicazione al Ministero del lavoro e delle politiche sociali e al Garante, stabilendo altresì che gli interessati, nel rivolgersi a (o se contattati da) un *call center*, siano sempre informati del fatto che l'operatore possa essere collocato in un Paese estero. Sono al riguardo pervenute, da parte delle imprese e delle associazioni di categoria, richieste di chiarimenti nonché di intervento del Garante per verificare le modalità di trattamento.

Nel contempo la Commissione europea è intervenuta nei confronti dell'Italia con una richiesta di informazioni, trasmessa al Garante dalla Presidenza del Consiglio dei Ministri, volta a verificare la sussistenza di eventuali presupposti per un'infrazione comunitaria in conseguenza delle possibili antinomie rilevate nel citato art. 24-*bis*, con particolare riguardo alla restrizione della libertà di srabilimento che l'applicazione della norma comporterebbe. Al riguardo sarebbe auspicabile un tempestivo intervento del legislatore tale da assicurare, in ragione di rilievi sollevati una formulazione della norma coerente con il diritto comunitario.

Con il provvedimento del 10 ottobre 2013, n. 444 (doc. web n. 2724806) il Garante ha comunque fornito indicazioni e chiarimenti, per i profili di propria competenza, anche in relazione agli strumenti da adottare per trasferire lecitamente dati personali verso Paesi terzi nonché sugli adempimenti espressamente previsti dall'art. 24-*bis*, prescrivendo ai titolari del trattamento di comunicare all'Autorità ogni trasferimento o affidamenro di dati personali a *call center* siti al di fuori dell'Unione europea; ciò anche al fine di consentire all'Autorità di effettuare una ricognizione del fenomeno disponendo di dati completi che riguardino tutti i settori pubblici e privati coinvolti, nonché per arginare efficacemente il fenomeno delle chiamate indesiderate.

Rispetto alle poco meno di 40 notificazioni ad oggi pervenute l'Autorità, pur non avendo ricevuto segnalazioni, ha tuttavia programmato un'attività ispettiva *ad hoc* per il 2014 al fine di verificare in concreto il rispetto delle vigenti disposizioni.

### 10.6. *I dati personali utilizzati a fini di profilazione e* marketing

Con riguardo ai trattamenti effettuati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico per finalità di profilazione della propria clientela attraverso l'uso di dati personali aggregati e senza l'acquisizione dello specifico consenso, il Garante ha analizzato una nuova istanza di verifica preliminare pervenuta da parte di un operatore telefonico sulla base del provvedimento generale del 25 giugno 2009 (doc. web n. 1629107). All'esito della stessa, l'Autorità ha emanato un provvedimento con il quale, nel prescrivere misure e accorgimenti (sia giuridici,

sia tecnici) volti a garantire, nell'ambito dell'attività di profilazione, il corretto utilizzo dei dati personali degli utenti ed a rafforzarne la tutela (provv. 24 ottobre 2013, n. 468, doc. web n. 2797824), si è consentito all'operatore telefonico in questione, previa adozione di rigorose misure di sicurezza, di ampliare i parametri utilizzati per la definizione della propria clientela e conseguentemente per la definizione di più idonei *cluster* (gruppi omogenei) di utenza sui quali articolare l'attività di profilazione. Inoltre, a fronte delle difficoltà rappresentate dall'operatore con riguardo ad una corretta ed adeguata gestione dei cicli di fatturazione, e soprattutto al fine di tutelare gli utenti a cui potevano essere imputati comportamenti di consumo non veritieri, l'Autorità ha anche autorizzato un'estensione del periodo di riferimento utilizzato per l'elaborazione del criterio di ripartizione della clientela nei suddetti *cluster*. Al fine di garantire gli utenti, l'Autorità non ha ritenuto invece lecita una nuova modalità di profilazione ipotizzata, nell'ambito di un'istanza di verifica preliminare, da una società di telecomunicazioni sulla base del monitoraggio dei dati di navigazione degli stessi (provv. 13 giugno 2013, n. 300). L'attività sottoposta al vaglio del Garante riguardava la cosiddetta pubblicità comportamentale (*targeted advertising*) e i servizi personalizzati su internet. La società fornitrice del servizio di connessione chiedeva infatti di poter analizzare il comportamento *online* degli utenti, senza averne acquisito il consenso, al fine di proporre pubblicità mirate (*targeted advertising*). Diversamente da quanto prospettato, è tuttavia emerso che il processo che avrebbe dovuto rendere anonimi i dati dei singoli utenti era, per sua natura, reversibile e consentiva di proporre all'utente offerte calibrate sulla sua condotta *online*.

Alla medesima società l'Autorità ha consentito, invece, nell'ambito di un'ulteriore istanza di verifica preliminare relativa alla fornitura di servizi di tv interattiva, di analizzare, previa acquisizione del consenso, il comportamento degli utenti e, in particolare, preferenze, gusti e scelte di consumo sui servizi e prodotti fruibili attraverso le piattaforme televisive digitali ed internet (provv. 11 aprile 2013, n. 177). A tal fine, sono state prescritte misure a tutela della riservatezza degli interessati, quali l'esclusione, per finalità di profilazione e *marketing*, dell'analisi di dati sensibili, a meno che il trattamento di tali dati non risultasse indispensabile in rapporto ad uno specifico bene o prodotto richiesto o, ancora, l'adozione, nella fase di classificazione dei prodotti televisivi fruibili in modalità interattiva, di una più ampia categorizzazione dei contenuti per genere (e che comunque non si riferisse a singole tipologie di contenuti digitali) nonché la previsione di un periodo di osservazione di gusti e preferenze di consumo non inferiore alla settimana.

Nel corso dell'istruttoria è emerso, inoltre, che la società avrebbe utilizzato, per l'analisi delle abitudini di consumo dei clienti della tv interattiva, la medesima piattaforma *software* usata per i servizi di telefonia e di profilazione telefonica. Pertanto, al fine di scongiurare i rischi di una "profilazione incrociata", il Garante ha prescritto il mascheramento dei dati personali all'interno dei diversi sistemi (provv. 11 aprile 2013, cit.).

### 10.7. *Il trattamento dei dati personali per finalità di* marketing *diretto: la manifestazione del consenso*

Dopo una articolata attività istruttoria volta a verificare la liceità e la correttezza dei trattamenti effettuati dai maggiori operatori nazionali di telefonia con riguardo ai dati personali dei clienti acquisiti sulla base del consenso (manifestato all'atto della sottoscrizione di un contratto di abbonamento o dell'attivazione di una linea prepa-

gata), il Garante è intervenuto con un provvedimento generale (15 maggio 2013, n. 242, doc. web n. 2543820) in tema di manifestazione del consenso nell'ambito del cd. *marketing* diretto; con esso sono state dettate alcune prescrizioni, successivamente ribadite con le linee guida in materia di attività promozionale e contrasto allo *spam* del 4 luglio 2013 (di cui, più nel dettaglio, v. *infra* par. 10.10). In particolare, con il menzionato provvedimento del 15 maggio 2013 – che (pur originato nel contesto degli operatori telefonici) si rivolge a tutti i titolari che effettuano trattamenti di dati personali in ambito privato – l'Autorità ha delineato, nel rispetto dei principi di semplificazione, armonizzazione ed efficacia di cui all'art. 2, comma 2, del Codice, una linea interpretativa dell'art. 130, commi 1 e 2, del Codice in relazione al disposto dell'art. 23, tesa a semplificare l'acquisizione del consenso dell'interessato per l'attività di *marketing* diretto attraverso strumenti tradizionali e automatizzati di contatto (posta elettronica, telefax, messaggi del tipo mms o sms o di altro tipo). In particolare, il Garante ha chiarito che l'acquisizione del consenso degli interessati per il trattamento dei dati personali per finalità di *marketing* diretto (ossia per l'invio di materiale pubblicitario, di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale), tramite modalità automatizzate ai sensi dell'art. 130, commi 1 e 2, del Codice, implica altresì il consenso alla ricezione di comunicazioni promozionali attraverso modalità tradizionali, come la posta cartacea o le chiamate telefoniche tramite operatore, salvo l'esercizio da parte dell'interessato del diritto di opposizione al trattamento (anche in forma parziale, limitatamente a talune modalità dell'attività di *marketing*).

Il Garante ha inoltre chiarito che dall'informativa deve emergere che il diritto di opposizione dell'interessato al trattamento per finalità di *marketing* diretto attraverso modalità automatizzate si estende a quelle tradizionali, anche se deve comunque restare salva la possibilità di esercitare tale diritto in parte, così come previsto dal citato art. 7, comma 4, del Codice. La stessa informativa deve infatti evidenziare la possibilità per l'interessato di manifestare comunque in maniera agevole e gratuita l'eventuale volontà di ricevere comunicazioni promozionali esclusivamente attraverso modalità tradizionali, ove previste. L'Autorità ha infine prescritto ai titolari del trattamento che per le menzionate finalità abbiano già raccolto un unico consenso con riguardo a comunicazioni sia automatizzate sia tradizionali, di inserire un analogo richiamo alla suddetta possibilità in un'informativa da rendere alla prima occasione utile, eventualmente anche mediante le ordinarie modalità di contatto per scopi endocontrattuali.

Con lo scopo di chiarire l'ambito di un corretto trattamento dei dati personali anche rispetto alla formulazione di una modulistica relativa sia all'informativa (*ex* art. 13 del Codice), sia al consenso (*ex* art. 23 del Codice) in termini selettivi, ovvero che consenta di prestare un consenso specifico per ogni finalità perseguita dal titolare, l'Autorità è intervenuta anche con riguardo ai trattamenti di dati personali svolti per finalità di *marketing* diretto da società che operano nel settore dei finanziamenti privati. In tale ambito, con riguardo alla comunicazione dei dati a soggetti terzi sempre per finalità di *marketing*, l'Ufficio, per garantire agli interessati confini più chiari dell'ambito in cui i loro dati vengono trattati, ha rilevato che il titolare, nel rendere un'idonea informativa, circa gli elementi di cui al citato art. 13, deve indicare, ove opportuno, tra i soggetti terzi destinatari della comunicazione anche le società controllate, controllanti o comunque a vario titolo collegate con il soggetto che ha raccolto i dati, ovvero, in alternativa le categorie merceologiche di appartenenza dei suddetti terzi (note 3 e 12 dicembre 2013).