Tali studi prevedono, in particolare, che informazioni trattate a fini amministrativi dai comuni siano trasmesse dalle regioni e dalle province autonome al sistema informativo dell'Inps, corredate di dati identificativi diretti e di dati molto delicati relativi anche allo stato di salute e alla vita sessuale. In entrambi i casi tra gli obiettivi dello studio vi sarebbe quello di far confluire i predetti flussi informativi nel Casellario dell'assistenza istituito presso l'Inps ai sensi dell'art.13 del d.l. 31 maggio 2010, n. 78, convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 30 luglio 2010, n. 122, le cui modalità di attuazione dovranno essere definite con un decreto del Ministro del lavoro e delle politiche sociali, di concerto con il Ministro dell'economia e delle finanze, nel rispetto del Codice.

In tale quadro, il Garante si è riservato di valutare, nell'ambito del parere di conformità sul decreto attuativo del Casellario dell'assistenza, la compatibilità con la normativa in materia di protezione dati di un'eventuale raccolta centralizzata -con dati identificativi diretti, in un unico sistema- di informazioni così delicate, anche idonee a rivelare lo stato di salute e la vita sessuale, riferite a minori. Ciò, anche con riferimento all'attuazione dei nuovi flussi di dati personali in ambito sociale e assistenziale previsti dall'art. 16 del d.l. 9 febbraio 2012, n. 5, convertito in legge, con modificazioni, dalla l. 4 aprile 2012, n. 35.

In particolare l'Autorità ha evidenziato che i dati personali trattati per scopi statistici non possono essere utilizzati per finalità di altra natura e che i relativi prospetti identificativi non indicano l'assenza dell'obbligo di risposta da parte degli interessati con riferimento ai dati sensibili e giudiziari, il trattamento dei quali, per altro, allo stato non è previsto da alcuna norma di legge che individui i tipi di dati e le operazioni eseguibili.

L'Autorità ha pertanto condizionato il parere favorevole sul Psn 2011-2013, Aggiornamento 2013, all'eliminazione dallo stesso dei predetti studi progettuali del Ministero del lavoro e delle politiche sociali (parere 20 settembre 2012 [doc. web n. 2069239]).

Informativa semplificata

Per la realizzazione del Censimento, l'Istat si è avvalsa delle liste anagrafiche comunali (lac) per acquisire i contatti necessari all'inoltro dei questionari censuari e ridurre il numero di rilevatori impiegati sul campo. In base alla normativa di settore, trattandosi di dati personali non raccolti presso l'interessato, ove il conferimento dell'informativa a quest'ultimo richieda uno sforzo sproporzionato rispetto al diritto tutelato, l'informativa stessa si considera resa se

il trattamento è incluso nel Psn o è oggetto di pubblicità con idonee modalità da comunicare preventivamente al Garante, il quale può prescrivere eventuali misure ed accorgimenti (art. 6, comma 2, del codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistan). L'Istat ha dovuto avviare la rilevazione delle liste anagrafiche comunali -una raccolta di dati presso terzi- prima dell'approvazione del Psn 2011-2013 e, pertanto, ha comunicato al Garante di voler pubblicare un'apposita informativa su due giornali a larga diffusione nazionale e su un giornale locale per i cittadini italiani di lingua tedesca della Provincia autonoma di Bolzano. L'Autorità, tuttavia, ha ritenuto che l'informativa dovesse essere pubblicata anche sul sito internet dell'Istat e che dovesse rimanere visibile fino alla pubblicazione del Psn 2011-2013 nella Gazzetta Ufficiale (provv. 19 gennaio 2011 [doc. web n. 1784974]).

Della possibilità di fornire un'informativa semplificata si sono avvalsi nel 2012 anche alcuni soggetti Sistan.

In particolare, il Ministero dell'istruzione, dell'università e della ricerca ha rappresentato all'Autorità di voler realizzare uno studio statistico sul valore degli esiti degli esami di Stato con riguardo all'ingresso degli studenti nelle università, attraverso l'elaborazione di dati già in suo possesso raccolti in banche dati amministrative diverse (nota 2 marzo 2012).

L'Istat, invece, si è avvalso di tale possibilità per alcune notizie relative al ruolo di responsabili del trattamento svolto da alcune regioni compartecipanti al progetto "Sperimentazione di un nuovo flusso di acquisizione dei dati di mortalità"- STU IST 02150, già inserito nel Pns 2011-2013 e nel relativo Aggiornamento 2012-2013 (nota 26 luglio 2012), nonché per comunicare alla Banca d'Italia i nominativi di famiglie campione estratti dalle anagrafi comunali per un'indagine sui bilanci delle famiglie italiane (v. art. 21, comma 2, del Regolamento (CE) n. 223/2009, che autorizza la "trasmissione di dati riservati" da un'autorità del sistema statistico europeo (nella specie, l'Istat) a un membro del sistema europeo delle banche centrali (nella specie la Banca d'Italia) "*a condizione che sia necessaria ai fini dell'efficienza dello sviluppo, della produzione e della diffusione di statistiche europee o del miglioramento della loro qualità*" e "*che tale necessità sia stata giustificata*"). L'Autorità ha al riguardo precisato che l'origine dei dati trattati dovrà essere

specificata anche nell'informativa che la Banca d'Italia renderà agli interessati nell'ambito dello svolgimento della predetta indagine statistica campionaria sui bilanci delle famiglie italiane (nota 17 dicembre 2012).

Collaborazione con l'Istat

Nel 2012, l'Ufficio ha collaborato con l'Istat per la revisione dei prospetti identificativi dei progetti inseriti nel Psn utilizzati per descrivere il trattamento di dati personali al fine di rendere una corretta informativa agli interessati, con particolare riferimento alla comunicazione dei dati sensibili e giudiziari tra soggetti Sistan.

Infine il Garante ha manifestato all'Istat la propria disponibilità a partecipare alla revisione del d.lgs. n. 322 del 1989 e al complessivo riordino del Sistema statistico nazionale cui l'Istituto si accinge alla luce di recenti modifiche normative (nota 27 novembre 2012).

8. L'ATTIVITÀ DI POLIZIA

8.1. IL CONTROLLO SUL CED DEL DIPARTIMENTO DELLA PUBBLICA SICUREZZA

A seguito di segnalazioni ricevute, l'Autorità ha assicurato 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 della l. 1° aprile 1981, n. 121, come modificato dall'art. 175 del Codice.

8.2. ALTRI INTERVENTI IN RELAZIONE AD ATTIVITÀ DI FORZE DI POLIZIA

Nel 2012 si è conclusa una complessa istruttoria avviata a seguito di un quesito posto dal legale rappresentante di una struttura operante nel campo del recupero e reinserimento di soggetti tossicodipendenti, concernente la richiesta proveniente da un Comando dell'Arma dei Carabinieri di inviare l'elenco di tutte le persone accolte presso la struttura.

All'esito dell'istruttoria, esaminate le fonti normative, il Garante ha comunicato al rappresentante della struttura e al Comando dell'Arma che non risultava sussistere una base normativa idonea a giustificare la trasmissione sistematica al Comando dell'elenco delle persone ricoverate presso la comunità terapeutica, rilevando che tali informazioni possono essere legittimamente acquisite unicamente a puntuale evasione di richieste provenienti dall'autorità giudiziaria, finalizzate al controllo dei soggetti sottoposti a misure restrittive ed alternative della libertà personale eventualmente soggiornanti presso la comunità (nota 26 gennaio 2012).

È altresì pervenuta al Garante una segnalazione con la quale veniva riferito che un agente di polizia in borghese aveva effettuato videoriprese nel corso di una manifestazione, dall'esterno del corteo, nel quale si era successivamente inserito, effettuando riprese a distanza ravvicinata e captando anche suoni e conversazioni.

Il commissariato interessato, nel riscontrare la richiesta di chiarimenti dell'Autorità, ha precisato che, trattandosi di manifestazione non autorizzata, le riprese come previsto in tali circostanze, erano finalizzate unicamente a individuare eventuali autori di reati. Nel caso di specie le riprese avevano consentito di identificare una persona, nei cui confronti era stato

promosso un procedimento penale e che era stata rinviata a giudizio, quale autore di un'aggressione ai danni di un operatore di polizia. Il commissariato ha altresì chiarito che le riprese erano state dirette a riprendere le fasi dei tafferugli e non per captare anche suoni e conversazioni, e che le eventuali tracce sonore di sottofondo rilevate in tali circostanze non erano riconducibili a persone definite.

Sulla base di tali chiarimenti il Garante non ha ravvisato violazioni della disciplina in materia di protezione dei dati personali nell'attività posta in essere dagli agenti, rientrante nell'ambito dei trattamenti effettuati dalle forze di polizia, ai sensi degli artt. 53 e ss. del Codice, per finalità di tutela dell'ordine e della sicurezza pubblica (nota 4 maggio 2012).

Non sono emerse violazioni neppure riguardo ad una segnalazione con cui veniva riferito che le postazioni informatiche presenti nella sala intercettazione di un comando dell'Arma dei Carabinieri risultavano sprovviste di *password* e che conseguentemente era possibile per chiunque si trovasse nella sala accedere liberamente alla documentazione ivi presente. Nel caso di specie, il segnalante, in servizio presso il comando dell'Arma, aveva avuto casualmente accesso ad un documento contenente una relazione di servizio che lo riguardava.

Il Comando, interpellato dall'Autorità, ha chiarito che la postazione informatica in questione, collegata ad una rete protetta e dotata di antivirus ad aggiornamento automatico, non era utilizzata per attività di intercettazione, ma era posta a disposizione del personale operante nella sala per ricerche di carattere personale su internet. Gli altri apparati presenti nella sala, utilizzati per attività di intercettazione, erano invece accessibili solo mediante procedure di autenticazione. Il Comando ha aggiunto che anche nel procedimento penale instaurato su denuncia-querela dell'interessato, conclusosi con un decreto di archiviazione, era stato accertato che l'evento rappresentato dal segnalante si era verificato su di una postazione non utilizzata per attività di intercettazione, e che era riconducibile ad un automatismo indotto da un *software* installato nel computer (nota 16 novembre 2012).

Accesso della polizia giudiziaria a dati sensibili

Un ufficio periferico dell'Inps ha chiesto a questa Autorità di conoscere le corrette modalità di comportamento in caso di richieste della polizia giudiziaria, finalizzate alla prosecuzione delle indagini, di accesso ai dati personali contenuti nei verbali di invalidità civile contenenti l'indicazione delle patologie.

Il Garante ha ricordato che tale ipotesi è regolata dall'art. 25, comma 2, del Codice -applicabile anche ai trattamenti effettuati dai soggetti pubblici, in base al rinvio di cui all'art. 18, comma 5, del Codice stesso- che, tra l'altro, consente la comunicazione di dati richiesti, in conformità alla legge, dalle forze di polizia per finalità di prevenzione, accertamento o repressione di reati (nota 21 novembre 2012).

Accertamento della situazione economica del debitore prodromica a procedura esecutiva

Un cittadino aveva segnalato di essere stato convocato da un commissariato della polizia di Stato, in quanto debitore delle spese di giudizio relative ad un contenzioso con una pubblica amministrazione, al fine di acquisire notizie sulla sua situazione economica, in previsione dell'eventuale promozione di una procedura esecutiva a suo carico.

Al riguardo il Garante ha osservato che l'ordinamento giuridico prevede appositi strumenti per consentire al creditore esecutante di individuare i beni del debitore da sottoporre a pignoramento (v. art. 492, comma 7, c.p.c.), mentre tra i compiti istituzionali della polizia di Stato non rientra il compimento delle suddette indagini; né, nella specie, risulta applicabile l'art. 53 del Codice, che ha riguardo al trattamento di dati personali effettuato per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, nella specie non ricorrenti.

Né il trattamento né la comunicazione dei dati all'ente pubblico esecutante risultavano quindi previsti da idonea base normativa, ovvero rientranti nelle funzioni istituzionali della polizia, sicché sono risultati violati gli artt. 18, comma 2 e 19 comma 2, del Codice.

Per questi motivi il Garante ha dichiarato illecito il trattamento e vietato, ai sensi degli artt. 143, comma 1, lett. *c)* e 154, comma 1, lett. *d)*, del Codice, ogni ulteriore operazione di trattamento di tali dati da parte del commissariato e dell'ente pubblico creditore, salva la valutazione della sussistenza dei presupposti per la contestazione di violazioni amministrative (provv. 4 ottobre 2012).

8.2.1. Acquisizione di dati da parte delle forze di polizia

Nel 2012 il Ministero dell'interno ha sottoposto al Garante, per il parere "conforme", ossia obbligatorio e vincolante previsto dall'art. 54 del Codice, due convenzioni volte a disciplinare l'accesso per via telematica delle forze di polizia a due importanti banche dati.

Convenzione tra il Ministero dell'interno e l'Inps

Il primo parere era stato richiesto dal Dipartimento della pubblica sicurezza del Ministero dell'interno in ordine a uno schema di Convenzione avente a oggetto l'accesso da parte delle forze di polizia, tramite il Centro elaborazione dati (Ced) del Dipartimento, alla banca dati dell'Inps, attraverso l'utilizzo di specifiche applicazioni informatiche. In entrambi i casi i testi sono stati definiti sulla base di approfondimenti svolti dall'Autorità con le parti, in un clima di piena collaborazione, per assicurare il rispetto, anche sotto il profilo della sicurezza, delle norme sulla protezione dei dati personali.

La prima richiesta è risultata fondata sulla normativa (l. 31 maggio 1965, n. 575, confluita nel codice delle leggi antimafia d.lgs. n. 159/2011) che prevede, tra l'altro, da parte dei questori, sia l'adozione di misure di prevenzione nei confronti degli indiziati di appartenere alla criminalità organizzata sia, anche a mezzo della Guardia di finanza o della polizia giudiziaria, che agisce anche ai sensi dell'art. 55 c.p.p., lo svolgimento di indagini sul tenore di vita, sulle disponibilità finanziarie e sul patrimonio di tali soggetti.

A tali fini il questore può richiedere ad ogni ufficio della p.a., ad imprese, società ed enti di ogni tipo, informazioni e copia della documentazione ritenuta utile.

Il testo definisce in particolare quali dati siano oggetto della Convenzione (dati anagrafici, retributivi, contributivi e pensionistici dei soggetti censiti dall'Inps), le finalità dell'accesso (esclusivamente quelle connesse allo svolgimento delle attività previste dalla suddetta normativa) ed il personale ad esso abilitato (operatori delle forze di polizia con qualifica di ufficiale o agente di polizia giudiziaria), cui dal Ced sono attribuiti specifici profili di abilitazione e credenziali di autenticazione personali ed impartite direttive relative alle responsabilità connesse all'uso illegittimo delle informazioni.

È altresì previsto, per entrambe le parti, l'obbligo di formazione di detto personale all'utilizzo della banca dati; sono stati configurati specifici divieti a carico del Ced, in materia di duplicazione delle informazioni acquisite per la creazione di autonome banche dati e di utilizzo di dispositivi automatici (*robot*) che consentono la consultazione in forma massiva dei dati personali; per quanto concerne la sicurezza nel flusso dei dati è previsto l'utilizzo del protocollo "ssl" per garantire le funzionalità di crittografia dei dati trasferiti da *client* e *server*; il Ced sottopone l'accesso alla banca dati dell'Istituto ai sistemi per il monitoraggio degli

accessi e di *alert* su anomalia in uso al Centro; i risultati di tali attività sono resi disponibili per i capi degli uffici per trenta giorni nel portale del Ced.

Il testo indica la necessità della consultazione del Garante nell'ipotesi di modifiche o integrazioni alla convenzione.

L'Autorità ha, peraltro, subordinato il proprio parere favorevole sulla Convenzione:

- alla riformulazione della nozione di "dato personale" alla luce delle modifiche che hanno sottratto le persone giuridiche, gli enti e le associazioni dall'ambito di applicazione della disciplina in materia di protezione dei dati personali (art. 4 del Codice, v. art. 40, comma 2, del d.l. 6 dicembre 2011, n. 201 convertito dalla l. 22 dicembre 2011, n. 214);

- all'indicazione che l'allegato B. della Convenzione, contenente l'analitica elencazione dei dati consultabili, costituisce parte integrante della medesima (parere 2 febbraio 2012 [doc. web n.1875293]).

Convenzione tra il Ministero dell'interno e il Ministero dell'economia e delle finanze

Il secondo parere ha riguardato la Convenzione tra il Ministero dell'interno e il Ministero dell'economia e delle finanze avente a oggetto l'accesso da parte delle forze di polizia, tramite il Centro elaborazione dati (Ced) del Dipartimento della pubblica sicurezza, ai dati e alle informazioni contenuti nel Sistema informatizzato di prevenzione amministrativa delle frodi sulle carte di pagamento (Sipaf) gestito dall'Ufficio centrale antifrode dei mezzi di pagamento (Ucamp) del Ministero dell'economia e delle finanze (v. norme sull'accesso del Dipartimento della pubblica sicurezza alle informazioni e ai dati contenuti nel sistema di prevenzione delle frodi sulle carte di pagamento l. 17 agosto 2005, n. 166 e del d.m. del Ministero dell'economia e delle finanze 30 aprile 2007, n. 112).

Anche in questo caso il testo individua specificamente le tipologie di dati e di informazioni oggetto della convenzione (attraverso il riferimento all'elenco contenuto negli artt. 6 e 7 del citato d.m. n. 112/2007); delimita le finalità dell'accesso (solo la prevenzione e repressione dei reati connessi all'utilizzo di carte di credito o di altri mezzi di pagamento) (v. parere reso dal Garante il 19 ottobre 2006 sullo schema del decreto attuativo della l. n. 166/2005 [doc. web n. 1353472]), riservato agli operatori delle forze di polizia cui sono attribuiti dal Ced specifici profili di abilitazione e credenziali di autenticazione personali.

È posto l'obbligo per il Ced di impartire al personale abilitato direttive relative alle

responsabilità connesse all'accesso improprio alla banca dati, all'uso illegittimo delle informazioni e alla loro indebita divulgazione, comunicazione e cessione a terzi.

Sono stati previsti specifici divieti a carico del Ced, in materia di duplicazione delle informazioni acquisite per la creazione di autonome banche dati e di utilizzo di dispositivi automatici (*robot*) che consentono la consultazione in forma massiva dei dati personali.

Per quanto concerne la sicurezza nel flusso dei dati, viene specificato che gli utenti accedono al Sipaf esclusivamente tramite VPN (*Virtual Private Network*) *site to site* su rete *SPC* con protocollo "*IPsec/tunnel*", utilizzando inoltre il protocollo "ssl" per garantire le funzionalità di crittografia dei dati trasferiti tra *client* e *server*.

È previsto che il Ced provvede al tracciamento delle attività all'interno del suo dominio di applicazione, mentre l'applicativo Sipaf provvede al tracciamento delle operazioni svolte dagli utenti.

Il Ced sottopone l'accesso alla banca dati Sipaf ai sistemi per il monitoraggio degli accessi e di *alert* su anomalia in uso al Centro; i risultati di tali attività sono resi disponibili per i capi degli uffici per trenta giorni nel portale del Ced.

Il testo indica, infine, la necessità della consultazione del Garante nell'ipotesi di modifiche o integrazioni alla convenzione.

Poiché tali modalità sono conformi alla disciplina in materia di protezione dei dati personali, ivi compreso il profilo della sicurezza, il Garante ha espresso parere favorevole sulla Convenzione (parere 12 luglio 2012 [doc. web n. 1915461]).

8.3. IL CONTROLLO SUL SISTEMA DI INFORMAZIONE SCHENGEN

Accertamenti disposti dal Garante

Il Ministero dell'interno-Dipartimento della pubblica sicurezza ha rappresentato l'opportunità di differire l'adempimento delle ultime misure prescritte dal Garante per rafforzare la sicurezza nel trattamento dei dati effettuati per l'attuazione della Convenzione di Schengen, in ragione sia delle innovazioni tecnologiche che verranno introdotte con la prossima 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 ha differito i termini per l'adempimento delle prescrizioni, che sono in corso di attuazione (provv. 24 gennaio 2013 [doc. web n. 2324763]).

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 hanno subito un lieve calo rispetto all'anno precedente.

Sono invece rimaste sostanzialmente stabili 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.

9. L'ATTIVITÀ GIORNALISTICA

9.1. MINORI

Anche nel periodo di riferimento non sono mancate occasioni di valutare come si atteggia in concreto il delicato rapporto tra la libertà di informazione e il diritto alla riservatezza e alla protezione dei dati dei minori, che ha come principale quadro di riferimento il Codice (artt. 50 e 136 e ss), il codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica, riportato nell'Allegato A.1. del Codice (in particolare all'art. 7) e la Carta di Treviso.

Le disposizioni citate, oltre a richiedere il rispetto dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico, prevedono che il diritto del minore alla riservatezza deve sempre essere considerato come primario rispetto al diritto di cronaca. Le medesime disposizioni prevedono altresì espressamente che, al fine di tutelarne la personalità, i giornalisti non rendano identificabili i minori coinvolti in fatti di cronaca.

Il Garante ha invocato tali princìpi nel caso relativo all'attentato di Brindisi, invitando gli organi di informazione e i siti web ad astenersi dalla pubblicazione di dettagli e immagini lesivi della dignità della minorenne deceduta, raccomandando, inoltre, particolare attenzione e senso di responsabilità nell'utilizzare foto messe in rete dai minori per condividere momenti della loro vita.

Analogo richiamo è stato effettuato dall'Autorità per la vicenda della bambina deceduta in un tragico incidente su una spiaggia francese, in questo caso anche al fine di tutelare gli altri minori componenti della famiglia della vittima (v. rispettivamente comunicati stampa 19 maggio e 28 agosto 2012 [doc. web nn. 1894787 e 1921070]).

Tanto più è necessaria la sensibilizzazione sul tema cronaca e minori e il rispetto delle garanzie sopra richiamate ove si consideri la diffusione illimitata (e talora dirompente) del web rispetto alle notizie di cronaca. Così è stato per il caso delle immagini e dei dati personali relativi al bambino di Padova prelevato a scuola dalle forze di polizia, in esecuzione di un provvedimento giurisdizionale di affidamento (comunicato stampa 11 ottobre 2012 [doc. web n. 2058275]).

Nell'ambito di alcuni riscontri forniti su segnalazioni pervenute nel corso dell'anno riguardanti la diffusione di immagini riferite a minori di età, l'Autorità, richiamando quanto affermato nel documento del 6 maggio 2004 "*Privacy* e giornalismo. Alcuni chiarimenti in risposta a quesiti dell'Ordine dei giornalisti" [doc. web n. 1007634], ha sottolineato che la diversità del contesto all'interno del quale possono essere raccolte e successivamente diffuse informazioni riguardanti i minori può influire significativamente sulla complessiva valutazione della pubblicazione stessa. In particolare, può risultare lecita la diffusione di immagini che danno positivo risalto a qualità del minore o che lo rappresentano in momenti di svago o di gioco (nota 29 agosto 2012).

9.2. CRONACHE GIUDIZIARIE

Nel 2012 una parte significativa delle richieste di intervento rivolte al Garante ha riguardato il trattamento di dati personali nell'ambito della cronaca giudiziaria che -nel necessario bilanciamento tra libertà di espressione, tutela della riservatezza e della dignità delle persone, anche alla luce dei princìpi di non colpevolezza sino alla sentenza definitiva e di rieducazione del condannato- deve conformarsi sia alle disposizioni di cui agli artt. 136-139 del Codice, sia al codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica.

9.2.1. Pubblicazione di intercettazioni

L'applicazione dei suddetti princìpi impone particolari cautele in caso di pubblicazione di intercettazioni effettuate nell'ambito di procedimenti giudiziari, anche alla luce della specifica aspettativa di riservatezza riconosciuta a coloro che sono impegnati in una conversazione telefonica o in altra forma di comunicazione in ambito privato.

In concreto, risulta spesso difficile per il Garante, sulla base della documentazione disponibile, valutare la conformità di specifiche pubblicazioni alla disciplina in materia di segreto investigativo e divieto di pubblicazione di atti del procedimento penale. Anche alla luce di ciò, a fronte di un reclamo presentato da un componente parlamentare avverso la diffusione attraverso la rete internet del testo di un'informativa contenente la trascrizione di

numerose intercettazioni telefoniche che lo riguardavano, il Garante ha chiesto la collaborazione della procura della Repubblica competente per le relative indagini, al fine di accertare se il materiale oggetto di diffusione fosse o meno coperto da segreto (nota 18 dicembre 2012).

In un diverso caso, invece, l'Autorità ha ritenuto che non fosse stato travalicato il limite dell'essenzialità dell'informazione rispetto a fatti di interesse pubblico, in quanto la pubblicazione della notizia che una determinata utenza telefonica fosse stata sottoposta ad intercettazione era giustificata dalla presenza di rapporti tra l'intestatario dell'utenza e persone a diverso titolo legate ad una complessa indagine giudiziaria. Pertanto il Garante, anche alla luce del fatto che gli articoli giornalistici oggetto di segnalazione, al momento dell'accertamento dell'Ufficio, non risultavano rintracciabili all'interno dei motori di ricerca, ha ritenuto non vi fossero gli estremi per adottare provvedimenti di carattere inibitorio (nota 4 gennaio 2013).

9.2.2. Informazioni relative a procedimenti

Notizie e immagini di arrestati e indagati

L'Autorità ha fornito riscontro a diversi reclami e segnalazioni richiamando il principio, ormai consolidato, 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. 5, 6 e 12 del codice di deontologia). La valutazione deve essere fatta caso per caso, in prima battuta dal giornalista, nel quadro anche delle disposizioni che disciplinano il segreto delle indagini e il regime di pubblicazione degli atti processuali (artt. 114 e 329 c.p.p. e art. 684 c.p.).

Su tali basi sono state ritenute prive di fondamento diverse segnalazioni concernenti l'avvenuta pubblicazione dei nomi di persone indagate, imputate o condannate, effettuata nel rispetto dei princìpi posti dal Codice, in particolare dall'art. 137, comma 3 e dal codice di deontologia cit. (nota 29 agosto 2012).

L'Autorità ha d'altra parte confermato il proprio consolidato orientamento a tutela della dignità delle persone sottoposte a procedimento penale con il provvedimento 18 maggio 2012 [doc. web n. 1900914], in relazione alla segnalazione di un caso che presenta aspetti

di novità rispetto ad ipotesi prese in considerazione in passato. In particolare, nell'ambito di una trasmissione televisiva riconducibile al cd. "giornalismo di inchiesta", erano state diffuse immagini raccolte da agenti operanti in funzione di polizia giudiziaria, che in una irruzione notturna perquisivano gli appartamenti di alcuni indagati, procedendo alle operazioni di arresto.

Nel ritenere che il servizio televisivo avesse, in termini generali, lecitamente riferito gli esiti delle indagini coordinate dalla Direzione distrettuale antimafia, dando anche conto dei dati identificativi delle persone ad esse sottoposte, il Garante ha, invece, disposto il divieto dell'ulteriore diffusione delle immagini in chiaro riferite a queste ultime, ritratte all'interno delle proprie abitazioni private -anche attraverso l'utilizzo di cd. "primi piani"- nel momento delicatissimo della presa in consegna da parte delle forze dell'ordine, ritenendo che ciò avesse travalicato i limiti posti dall'ordinamento all'esercizio del diritto di cronaca, in particolare il principio di tutela della dignità della persona e il principio di essenzialità dell'informazione rispetto a fatti di interesse pubblico.

L'Autorità, inoltre, sempre a tutela della dignità delle persone arrestate, ha adottato un provvedimento inibitorio nei confronti di una maestra d'asilo arrestata per maltrattamento a danni di minori. L'immagine della stessa, al momento dell'arresto, infatti, veniva trasmessa nel corso di alcuni servizi giornalistici di telegiornali in relazione ad episodi di maltrattamenti a danno di minori non imputabili alla reclamante. Il Garante ha quindi ritenuto che, in tali casi, l'uso della suddetta immagine non potesse ritenersi essenziale rispetto alla finalità di fornire informazioni su un diverso episodio (provv. 5 giugno 2012 [doc. web n. 1912974]).

Vittime di reato, testimoni e persone estranee ai fatti

Il richiamato parametro dell'"*essenzialità dell'informazione*" ha costituito il principio-guida di riferimento nella valutazione di diversi trattamenti di dati, i quali, pur se attinenti a fatti giudiziari di rilevante interesse pubblico, includevano riferimenti a soggetti terzi la cui identità era meritevole di tutela (ad esempio familiari, anche minorenni, di persone interessate da procedimenti penali, parti lese); oppure riguardavano fatti che, pur essendo relativi alle persone indagate, risultavano essere estranei ai fatti oggetto di indagine.

In particolare il Garante, nell'esaminare alcuni reclami e segnalazioni in argomento, ha ribadito che nel trattamento di dati e immagini relativi a persone vittime di episodi

criminosi, il rispetto dell'"*essenzialità dell'informazione*" va assicurato con particolare rigore, anche quando le notizie riguardino vittime decedute.

Tali garanzie (che trovano riscontro anche nel quadro giuridico europeo: cfr. Raccomandazione (2003)13 del Comitato dei ministri del Consiglio d'Europa del 10 luglio 2003 "Princìpi relativi alle informazioni fornite attraverso i mezzi di comunicazione in rapporto a procedimenti penali") sono state richiamate, fra l'altro, a fronte della diffusione, da parte di alcuni giornali e siti di informazione, di immagini tratte dalla perizia medico legale effettuata sul corpo di una donna, che il Garante ha ritenuto eccedenti rispetto alla finalità informativa e lesive della dignità dell'interessata (note 9 agosto e 8 novembre 2012).

Le medesime garanzie di tutela sono state alla base della valutazione di una segnalazione relativa ad alcuni servizi giornalistici riguardanti il nuovo filone di indagine sulla morte di una giovane studentessa di Brembate, relativamente al possibile coinvolgimento di un uomo, poi defunto (le cui tracce di Dna lo qualificherebbero quale padre naturale del possibile omicida) e dei suoi familiari (autori della segnalazione). L'Autorità ha infatti ritenuto eccedente la pubblicazione della fotografia del defunto apposta sulla lapide nonché una serie di informazioni relative ai suoi familiari (dati anagrafici, di residenza e credo religioso) pubblicate, in particolare, da un quotidiano locale. Ciò, considerato che si trattava di un'ipotesi investigativa discussa, ancora alla fase iniziale, e che era emersa da subito l'estraneità del defunto e dei familiari citati dal giornale rispetto all'omicidio della giovane (nota 13 dicembre 2012).

Il Garante ha altresì ritenuto fondata la segnalazione di una donna che aveva lamentato una possibile lesione della sua *privacy* e della sua sicurezza personale in ragione della pubblicazione, all'interno di un quotidiano, della prima parte del verbale della sua deposizione quale "*persona informata di fatti*" oggetto di un procedimento penale. La riproduzione fotografica, con caratteri leggibili e senza alcuna forma di mascheramento, di parte di questo verbale aveva infatti reso conoscibili alcuni dati della segnalante (in particolare la data e il luogo di nascita nonché la attuale residenza, comprensiva di via e numero civico) che il Garante ha ritenuto non essenziali ai fini della completezza informativa sulla vicenda di interesse pubblico oggetto di quel procedimento penale (nota 16 luglio 2012).

9.3. PERSONAGGI PUBBLICI

L'Autorità è stata nuovamente chiamata ad affrontare la questione della raccolta e diffusione di informazioni riguardanti personaggi pubblici o persone che esercitano pubbliche funzioni. Come evidenziato nelle precedenti relazioni annuali, il quadro normativo e l'evoluzione giurisprudenziale in materia consentono di individuare margini più ampi nel trattamento dei dati personali relativi a siffatte figure. Lo stesso codice di deontologia stabilisce che "*la divulgazione di notizie di rilevante interesse pubblico o sociale non contrasta con il rispetto della sfera privata quando l'informazione, anche dettagliata sia indispensabile in ragione della....qualificazione del protagonista*" (art. 6, comma 1).

Dallo stesso codice si evince altresì che informazioni riguardanti personaggi pubblici, anche relative alla loro sfera privata, possono essere divulgate se assumono rilievo sul loro ruolo o sulla loro vita pubblica (art. 6, comma 2), ovvero se tratte da dichiarazioni o comportamenti pubblici degli stessi interessati (art. 137, comma 3 del Codice). Anche in tale ambito vanno comunque rispettati l'essenzialità dell'informazione e la dignità della persona (artt. 10 e 11 del codice di deontologia).

In tale quadro normativo l'Autorità ha ritenuto leciti alcuni articoli, oggetto di segnalazione, relativi al ricovero della presidente di una regione in una struttura sanitaria, per un intervento. Il Garante non ha rinvenuto in essi dettagli relativi alla patologia o al tipo di intervento subito o altre informazioni eccedenti; d'altra parte ha riscontrato che gli articoli facevano riferimento a una questione da cui aveva preso le mosse anche un'interrogazione consiliare e di cui non poteva non riconoscersi una rilevanza pubblica. Il Garante ha poi riscontrato che gli organi di informazione avevano dato anche ampia evidenza ai successivi chiarimenti dell'interessata sulla vicenda (nota 11 ottobre 2012).

I limiti sopra ricordati sono stati invece richiamati dal Garante in merito a un reclamo concernente la pubblicazione di servizi giornalistici relativi ad un'asserita relazione sentimentale tra due personaggi dello spettacolo, desumibile da uno scambio di sms, poi prodotti in un procedimento giudiziario. In particolare il Garante ha prescritto agli organi di informazione di astenersi dalla pubblicazione di sms eventualmente idonei a rivelare abitudini sessuali (art. 11 codice di deontologia) (provv. 13 dicembre 2012 [doc. web n. 2142715]).