

8 La ricerca scientifica e la statistica

8.1. *La ricerca scientifica*

L'autorizzazione generale n. 9 al trattamento di dati sensibili per finalità di ricerca scientifica – rinnovata fino a dicembre 2016 in termini sostanzialmente analoghi alla precedente (prov. 11 dicembre 2014, n. 591, doc. web n. 3632879) e sulla quale l'Ufficio ha fornito indicazioni generali allo scopo di promuovere una corretta attuazione delle disposizioni in materia di protezione dei dati personali – consente di trattare dati personali sulla salute (e, laddove siano indispensabili per il raggiungimento delle finalità della ricerca, dati sulla vita sessuale e sull'origine razziale ed etnica), in assenza del consenso dei pazienti interessati, per studi e ricerche in campo medico, biomedico e epidemiologico nel caso in cui risulti impossibile rendere l'informativa agli interessati, a causa, tra gli altri, di "motivi di impossibilità organizzativa". Ciò a condizione che sul progetto di ricerca si sia espresso favorevolmente, con parere motivato, il comitato etico territorialmente competente (artt. 107 e 110 del Codice).

In proposito, è stato precisato che, nelle ipotesi di "impossibilità organizzativa", è possibile utilizzare i dati personali dei soli pazienti i quali, all'esito di ogni ragionevole sforzo compiuto presso i centri di cura per contattarli (ad es., attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti o l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente), risultino essere deceduti o non contattabili al momento dell'arruolamento nello studio (nota 6 maggio 2014).

L'Autorità ha altresì affrontato il tema dei trattamenti di dati personali, anche sensibili, effettuati per la realizzazione e la tenuta di registri di patologia. Al riguardo, una Asl ha chiesto all'Autorità un'autorizzazione al trattamento dei dati sensibili per la gestione di un registro tumori provinciale. Nel fornire riscontro, l'Ufficio ha avuto occasione di chiarire che, alla luce della regolamentazione dettata dalla legge regionale (che prevede la realizzazione di un registro della popolazione regionale articolato su base provinciale e sub-provinciale), le finalità del trattamento sono riconducibili al perseguimento di scopi di ricerca scientifica finalizzata alla tutela della salute in campo medico, biomedico ed epidemiologico (artt. 107 e 110 del Codice), nonché di valutazione dell'appropriatezza e dell'efficacia dell'assistenza sanitaria erogata (art. 85 del Codice). Tali attività, previste dalla legge regionale tra quelle istituzionalmente perseguite dal registro, sono inoltre qualificate dal Codice di rilevante interesse pubblico (artt. 20, 85 e 98 del Codice).

Pertanto, ai fini della legittimità del trattamento è necessario individuare, con regolamento regionale, in conformità al parere espresso dal Garante, i tipi di dati sensibili e di operazioni indispensabili per l'espletamento delle predette attività, ivi compresi i soggetti che possono avervi accesso e i dati che possono conoscere, nonché le misure per la custodia e la sicurezza dei dati. Ciò in conformità alla disciplina del Codice sul trattamento dei dati sensibili e alle disposizioni legislative nazionali intervenute nel frattempo in materia di sistemi di sorveglianza e di registri di patologia (artt. 20 e 154 del Codice; art. 12, commi 10 ss., d.l. 18 ottobre 2012, n. 179 convertito con l. 17 dicembre 2012, n. 221). In questo quadro, l'Ufficio ha messo altresì in evidenza alcuni aspetti di criticità riscontrati nella disciplina regionale di

riferimento riguardo al trattamento dei dati personali degli ammalati di tumore da parte dei diversi soggetti coinvolti nel suo funzionamento (nota 1° dicembre 2014; v. sul punto anche parere 13 settembre 2012, n. 241, doc. web n. 1927415).

Sempre con riferimento al tema dei registri di patologia, l'Ufficio ha avviato un'attività di collaborazione con talune regioni che sono in procinto di disciplinare con proprio atto regolamentare i trattamenti di dati sensibili e, in particolare, di quelli attinenti alla salute, connessi alla tenuta e al funzionamento di registri tumori su base regionale (nota 14 gennaio 2015).

Un altro caso, esaminato dal Garante a seguito di accertamenti ispettivi avviati d'Ufficio, ha riguardato un registro gestito da un'associazione scientifica di medici nefrologi che a livello nazionale raccoglie dati sanitari riferiti a pazienti con insufficienza renale cronica per finalità di ricerca scientifica in campo medico-epidemiologico (prov. 16 gennaio 2014, n. 16, doc. web n. 2937031). Nell'ambito delle verifiche svolte, è emerso che il registro era alimentato, su base volontaria, dai responsabili dei registri regionali e provinciali di dialisi e trapianto, gestiti da enti e organismi sanitari pubblici, i quali inviavano all'associazione alcuni dati clinici disaggregati riferiti ai pazienti in trattamento dialitico presso i centri dialisi territoriali. I dati raccolti erano quindi elaborati e aggregati dall'associazione per analisi statistiche ed epidemiologiche e poi trasmessi a un'associazione europea per finalità di ricerca scientifica in ambito sovranazionale.

Dagli approfondimenti compiuti è stato riscontrato che tale trattamento avveniva in assenza di idonea informativa e del consenso degli interessati: l'associazione, infatti, riteneva che i dati raccolti fossero anonimi e che, quindi, questi non fossero soggetti alla disciplina in materia di protezione dei dati personali. Al contrario, l'Autorità ha accertato che i dati trasmessi dai registri territoriali, pur non contenendo i nominativi degli interessati, erano collegati allo stesso codice univoco con cui le informazioni erano memorizzate nel registro territoriale e riportavano numerose informazioni (ad es., data di nascita, sesso, codice della nefropatia, trattamenti dialitici effettuati, risultati degli esami clinici, patologie correlate alla malattia renale) che rendevano comunque possibile re-identificare i pazienti, sia pure mediante il collegamento con altri dati nella disponibilità di terzi.

Come è noto, le persone giuridiche private che perseguono finalità di studio e di ricerca scientifica possono utilizzare dati personali attinenti alla salute, anche raccolti presso strutture pubbliche, di regola a condizione di aver fornito una previa e idonea informativa agli interessati e aver ottenuto il loro specifico consenso (artt. 106, 107 e 110 del Codice e autorizzazione generale n. 2, punto 1.2). L'obbligo di raccogliere il consenso degli interessati non è richiesto solo in casi residuali, quando ricorrono particolari condizioni, quali la previsione dello specifico trattamento in una disposizione di legge, anche regionale, o l'essere inserito in un programma di ricerca biomedica o sanitaria, oppure quando non è possibile, a causa di particolari ragioni, informare gli interessati e il programma di ricerca è oggetto di parere favorevole del competente comitato etico ed è altresì autorizzato dal Garante.

Al riguardo, l'Autorità, nel sottolineare la rilevanza degli scopi di ricerca scientifica perseguiti dall'associazione, ha evidenziato che questi non possono prescindere dalla necessità di adottare adeguate misure a tutela della riservatezza degli interessati. È stato quindi vietato all'associazione di proseguire il trattamento dei dati sanitari dei pazienti nefropatici prima di aver provveduto ad informarli e ad acquisire il loro consenso nonché ad adottare adeguate misure di sicurezza per proteggere i dati. In alternativa, l'associazione potrà raccogliere dai centri dialisi territoriali solo dati "effettivamente anonimi" (art. 4, comma 1, lett. n), del Codice), non soggetti alla disciplina prevista dal Codice.

Infine, l'Autorità ha appreso da notizie di stampa che una regione ha regolato con propria delibera l'accesso alla banca dati sanitaria regionale da parte di enti esterni (pubblici e privati) affidatari dell'attività di valutazione dell'appropriatezza, dell'efficacia e dell'efficienza dell'assistenza sanitaria erogata, sulla base di una convenzione e dietro eventuale corresponsione di un contributo economico a titolo di rimborso dei costi sostenuti dall'ente regionale per la messa a disposizione del proprio patrimonio informativo.

Al riguardo, l'Ufficio ha curato specifici approfondimenti, anche nell'ambito di apposite riunioni con i responsabili dell'amministrazione, all'esito dei quali la regione ha comunicato all'Autorità di voler modificare e integrare il testo della propria delibera al fine di accogliere le indicazioni suggerite volte a rendere il testo conforme alla disciplina in materia di protezione dei dati personali. A tal fine, la regione si è impegnata a sottoporre all'Autorità il testo della nuova delibera e di ogni altro atto volto ad incidere sulla definizione della materia (nota 12 novembre 2014).

8.2. *La statistica*

Il d.l. 31 agosto 2013, n. 101, convertito con modificazioni in l. 30 ottobre 2013, n. 125, ha disposto l'abrogazione dell'art. 6-*bis*, comma 2, d.lgs. n. 322/1989, a tenore del quale "nel Programma statistico nazionale sono illustrate le finalità perseguite e le garanzie previste dal presente decreto e dalla legge 31 dicembre 1996, n. 675. Il Programma indica anche i dati di cui agli artt. 22 e 24 della medesima legge, le rilevazioni per le quali i dati sono trattati e le modalità di trattamento. Il Programma è adottato sentito il Garante per la protezione dei dati personali" (art. 8-*bis*, comma 1, lett. *a*).

Sulla base di tale abrogata disposizione, l'Istat, prima dell'adozione dei Psn, ha acquisito annualmente il parere del Garante, apportando ai Programmi stessi, ove necessario, le opportune modifiche indicate dall'Autorità affinché nell'ambito dei trattamenti di dati personali, anche sensibili e giudiziari, effettuati per finalità statistiche ivi descritti fosse garantito il più elevato livello di tutela dei diritti, delle libertà fondamentali e della dignità degli interessati, con particolare riferimento alla loro riservatezza, identità personale e al diritto alla protezione dei dati personali (art. 2 del Codice).

Inoltre, il rispetto della procedura prevista dall'abrogato art. 6-*bis*, comma 2, d.lgs. n. 322/1989, costituiva anche idoneo presupposto di legittimità per il trattamento di dati sensibili e giudiziari effettuato nell'ambito dei lavori statistici previsti dal Psn, alternativo alle regole generali poste dal Codice per il trattamento di tali categorie di dati personali (artt. 20-22 del Codice).

Ciò premesso, l'Istat, istituzionalmente tenuto a provvedere all'esecuzione delle rilevazioni statistiche previste nel Psn (art. 15, comma 1, lett. *b*), d.lgs. n. 322/1989), in un'ottica di semplificazione e anche al fine di garantire il rispetto delle specifiche garanzie previste per il trattamento dei dati sensibili e giudiziari, acquisiti i pareri del Ministero per la semplificazione e la pubblica amministrazione, del Comstat e della Commissione per la garanzia della qualità dell'informazione statistica (art. 12, d.lgs. n. 322/1989 e art. 3, d.P.R. n. 166/2010), ha avanzato al Garante la proposta di inserire nel codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, All. A.3. al Codice, adottato con provv. 31 luglio 2002, n. 13 (doc. web n. 1556573) un nuovo articolo 4-*bis*, in base al quale "nel Programma statistico nazionale sono illustrate le finalità perseguite e le garanzie previste dal d.lgs. 6 set-

tembre 1989, n. 322 e dal d.lgs. 30 giugno 2003, n. 196 e dal presente codice deontologico. Il Programma indica altresì i dati di cui all'art. 4, comma 1, lett. *d*) ed *e*), d.lgs. 30 giugno 2003, n. 196, le rilevazioni per le quali i dati sono trattati e le modalità di trattamento. Il Programma è adottato, con riferimento ai dati personali, sensibili e giudiziari, sentito il Garante per la protezione dei dati personali, ai sensi dell'art. 154 del d.lgs. 30 giugno 2003, n. 196". Ciò in quanto il citato codice di deontologia reca la disciplina del trattamento di dati personali effettuato dai soggetti che fanno parte del Sistema statistico nazionale, in particolare per quanto riguarda il trattamento dei dati sensibili e giudiziari indicati nel Psn, e considerato che il rispetto delle disposizioni contenute nel codice di deontologia è condizione essenziale per la liceità del trattamento dei dati personali (artt. 12, 106 e 108 del Codice).

Al riguardo, il Garante, considerati i ruoli del Comstat, della Commissione e dell'Istat in relazione all'adozione del Psn, ha condiviso la proposta di modifica del codice di deontologia presentata, nel rispetto del principio di rappresentatività, dai soggetti maggiormente interessati nella predisposizione del Psn (art.12 del Codice; artt. 12, comma 1, lett. *c*), 13, comma 3, e 15, comma 1, lett. *a*) e *b*), d.lgs. n. 322/1989; art. 5, comma 1, d.P.C.M. 28 aprile 2011; art. 3, comma 6, d.P.R. n. 166/2010). Nel merito, l'Autorità ha poi ritenuto che detta modifica consenta al Garante di poter effettuare le valutazioni di competenza relative al rispetto della disciplina in materia di protezione dei dati personali, con particolare riferimento alle garanzie previste per il trattamento dei dati sensibili e giudiziari (art. 22 del Codice). Su tali basi, ai sensi dell'art. 12, comma 2, del Codice, l'Autorità ha disposto l'integrazione del codice di deontologia con il sopra richiamato articolo 4-*bis*, rubricato "Trattamento di dati personali, sensibili e giudiziari, nell'ambito del Programma statistico nazionale" (prov. 12 giugno 2014, n. 296, doc. web n. 3268032).

Alla luce delle riforme normative sopra evidenziate, il Garante ha reso il parere di competenza sullo schema di Programma statistico nazionale 2014-2016 (di seguito Psn) ai sensi dell'art. 4-*bis* del codice di deontologia.

Anche tale parere, favorevole, è stato emanato all'esito di un'intensa collaborazione con l'Istat, volta a garantire un elevato *standard* di tutela del diritto alla protezione dei dati personali nell'ambito dei trattamenti effettuati per lo svolgimento dei lavori della statistica ufficiale (prov. 26 giugno 2014, n. 324, doc. web n. 3320710). In particolare, in tale Psn, l'Istat ha recepito le indicazioni dell'Ufficio in relazione all'informativa da rendere agli interessati ai sensi dell'art. 13 del Codice e 6, comma 2, del codice di deontologia, integrandola con i necessari chiarimenti in relazione alle singole componenti di cui essa deve essere composta (artt. 13 e 22, comma 2, del Codice). Come negli anni precedenti, il Psn prevede che l'informativa sia contenuta in un paragrafo del programma, oltre che nei singoli prospetti identificativi dei lavori statistici, fermo restando l'obbligo di fornire preventivamente idonea informativa agli interessati per le rilevazioni che prevedono la raccolta diretta di dati personali presso gli stessi.

In tale ambito, sono altresì state evidenziate le specifiche indicazioni in relazione alla "natura obbligatoria o facoltativa del conferimento dei dati". In particolare, nel ribadirsi che non sussiste obbligo di risposta per i dati sensibili e giudiziari – a meno che esso non sia previsto da un'espressa disposizione normativa –, è stato precisato che, nelle ipotesi di lavori statistici che comportano la raccolta presso soggetti terzi delle predette categorie di dati personali, è garantita, attraverso l'adozione di specifiche misure organizzative, la possibilità per l'interessato di aderire facoltativamente al trattamento statistico delle predette informazioni. Tale circostanza è stata, inoltre, opportunamente richiamata anche nei singoli prospetti identificativi, fatta eccezione per quelli inerenti ai lavori statistici che prevedono la raccolta di dati perso-

nali direttamente presso gli interessati e per quelli per i quali l'obbligo di risposta non sussiste in ogni caso: "indagini dirette collegate" effettuate nell'ambito degli Studi progettuali (identificati con la sigla Stu), Statistiche derivate o rielaborazioni (Sde) e per i Sistemi informativi statistici (Sis).

Facendo seguito alla raccomandazione resa dal Garante nel parere sul Psn 2011-2013, aggiornamento 2013 (cfr. parere 20 settembre 2012, n. 249, doc. web n. 2069239), il Psn fornisce idonei chiarimenti sul ruolo dei cd. "compartecipanti", distinguendo quanti collaborano alla realizzazione del lavoro, senza tuttavia trattare dati personali, da coloro che realmente sono coinvolti nelle operazioni di trattamento, questi ultimi, come evidenziato nel Programma, designati responsabili del trattamento ai sensi dell'art. 29 del Codice.

Sulla base delle indicazioni dell'Ufficio, l'Istat, al fine di informare adeguatamente gli interessati circa le finalità statistiche perseguite, laddove necessario ha riformulato, in termini più chiari, la descrizione dell'obiettivo statistico (art. 13, comma 1, lett. a), del Codice; ad es., IST-02546 *Micro demographic accounting* (MIDEA); EMR-00021 Sistema informativo della popolazione da circolarità anagrafica- sistema ANA-CNER; IPS-00020 Certificati di diagnosi per indennità di malattia; IST-02507 Analisi ai fini statistici delle Anagrafi nazionali degli studenti delle scuole e delle università; IPS-00042 Lavoratori parasubordinati; PBL-00004 SIS-Belluno: Sistema statistico sul mercato del lavoro; IPS-00009 Prestazioni dell'assicurazione contro la tubercolosi; IST-02481 Rilevazione integrativa sugli scambi con l'estero di merci e servizi).

Con riferimento all'analisi dei singoli lavori statistici si evidenzia, in primo luogo, che è stata posta particolare attenzione ad una nuova tipologia di lavoro consistente nella realizzazione di cd. *Repository*. Trattasi di basi di dati integrate (archivi amministrativi e fonti statistiche) volti alla realizzazione di archivi statistici intermedi, utili all'Istat per svolgere successive elaborazioni, anche di tipo longitudinale, nei diversi settori di interesse (ad es., IST-02520 Sviluppo di archivi statistici intermedi su unità socio-economiche - SIM; IST-02264 Base integrata di microdati statistici per l'analisi dell'occupazione; Sistema di integrazione logico-fisica di microdati amministrativi e statistici-SIM IST-02270).

Al riguardo, è stato ribadito (cfr. pareri 10 giugno e 23 settembre 2010, rispettivamente doc. web nn. 1734415 e 1753181) che i dati sensibili e giudiziari contenuti in elenchi, registri e banche dati devono essere resi momentaneamente inintelligibili anche a chi è autorizzato ad accedervi, permettendo l'identificazione degli interessati solo in caso di necessità e che i dati idonei a rilevare lo stato di salute e la vita sessuale devono essere conservati separatamente da altri dati personali che non richiedono il loro utilizzo (art. 22, commi 6 e 7, del Codice).

In secondo luogo, l'Istat, nel recepire le indicazioni dell'Ufficio, nei prospetti identificativi relativi a due lavori statistici inerenti, rispettivamente, la sindrome dell'Aids e il virus dell'HIV, considerato che tra i principali caratteri statistici rilevati vi sono anche i "fattori di rischio", ha evidenziato tra i dati sensibili trattati, anche quelli idonei a rivelare la vita sessuale, precisando, al contempo, la definizione di "fattori di rischio" (contatto eterosessuale o contatto omosessuale) (ISS-00004 Registro nazionale aids; ISS-00043 Sistema di Sorveglianza delle nuove diagnosi di infezione da HIV).

Con riferimento, infine, ai lavori statistici che prevedono la raccolta presso soggetti minori di età di dati sensibili o comunque inerenti aspetti particolarmente intimi della vita privata degli stessi idonei ad incidere sulla loro dignità (es. struttura familiare, soddisfazione vita quotidiana; condizioni di salute; tipo di esperienze sentimentali/sexuali, eventuali molestie, metodi anticoncezionali; intervalli di tempo

di lavoro retribuito; grado di soddisfazione della vita quotidiana), anche facendo seguito alle precedenti raccomandazioni del Garante (parere 20 settembre 2012, n. 249, doc. web n. 2069239), l'Istat ha previsto, nel Psn in esame, che la raccolta delle informazioni relative a minori infraquattordicenni avvenga per il tramite dei genitori o di un adulto di riferimento che risponde per il minore. Per gli infradiciottenni, invece, la rilevazione viene effettuata attraverso PC o altri strumenti informatici che escludono la presenza di un intervistatore che potrebbe suscitare sentimenti di soggezione o imbarazzo nell'interessato.

Con provvedimento del 18 settembre 2014, n. 411 (doc. web n. 3458502) il Garante ha fornito, ai sensi dell'art. 4-*bis* del codice di deontologia, il parere di competenza sul Programma statistico nazionale 2014-2016 aggiornamento 2015-2016 (Psn). In particolare, il parere è stato reso in relazione al trattamento di dati personali inseriti per la prima volta nel Psn ed alle modifiche apportate ai prospetti ai lavori statistici che comportano il trattamento di dati personali già inclusi nel Psn 2014-2016.

In tale ambito, l'Autorità ha formulato alcune osservazioni in relazione a specifici lavori statistici. In particolare, sulla base delle indicazioni dell'Ufficio, l'Istat ha convenuto di modificare la scheda informativa relativa al lavoro statistico "Prestazioni economiche di malattia e maternità"-IPS-00052, specificando che esso comporta altresì, come si evince anche dalla denominazione dello stesso, il trattamento di dati sensibili idonei a rivelare lo stato di salute degli interessati.

Nell'ambito dell'attività istruttoria è stata inoltre posta particolare attenzione al lavoro statistico "Uso a fini statistici dei *Big Data*" IST-02589. Con tale locuzione l'Istat ha voluto fare riferimento ai dati di telefonia mobile, elaborati a fini di programmazione e gestione dei servizi locali e individuazione di opportune misure di protezione civile. In particolare, le informazioni di telefonia mobile trattate riguardano un sottoinsieme delle variabili registrate del gestore telefonico durante una chiamata, denominato *call detail record* (cdr). Il cdr è un "progressivo" (sostitutivo del codice fiscale, nome e cognome, corrispondente all'utente) al quale, per la rilevazione statistica, vanno aggiunte le informazioni relative al comune nel quale si trova la cella di effettuazione della chiamata, la data e ora della stessa.

Al riguardo, l'Istat su specifica richiesta dell'Ufficio, ha fornito idonee assicurazioni sulla natura anonima dei dati raccolti presso il gestore telefonico. A tal fine quest'ultimo assegna un codice ad ogni cdr eliminando successivamente ogni possibilità di raccordo tra tale codice e gli identificativi originali.

I *big data* rappresentano un ampio patrimonio informativo e l'utilizzo di queste informazioni comporta specifici rischi per l'effettiva tutela della riservatezza degli interessati e la corretta applicazione della disciplina in materia di protezione personali, tenuto anche conto che grazie alle nuove tecnologie e alle nuove tecniche di analisi, mediante l'elaborazione e l'interconnessione dei dati risulta possibile re-identificare un interessato anche attraverso informazioni apparentemente anonime (cd. *single-out*).

Su tali basi, è stata posta particolare attenzione anche all'analisi delle successive modalità di trattamento dei dati anonimi raccolti dall'Istat presso il gestore telefonico.

Al riguardo, l'Istituto ha precisato che la sperimentazione è volta a stimare i flussi intercomunalmente a livello aggregato e non individuale. In ordine, poi, all'eventuale rischio di re-identificazione derivante dalla possibilità di individuare un'unità elementare tramite collegamento – indiretto – ad altre fonti di dati in possesso dell'Istituto, su specifica richiesta dell'Ufficio è stata fornita idonea assicurazione che, nell'ipotesi in cui dovessero verificarsi frequenze di flusso inferiori a tre unità, le stesse verranno oscurate.

L'Istat ha infine precisato che i dati e le procedure descritte verranno utilizzate, con riferimento ai dati di telefonia mobile della sola provincia di Pisa nel mese di ottobre 2011, a fini esplorativi, di sperimentazione e messa a punto di applicativi per la stima di flussi aggregati che verranno in futuro gestiti direttamente dai gestori telefonici. L'Autorità si è riservata di effettuare verifiche anche in relazione ai trattamenti effettuati dai gestori telefonici.

Nell'ambito dei lavori volti a diffondere le stime di povertà ed esclusione sociale sono emerse alcune criticità in relazione al lavoro statistico "Povertà e deprivazione trasversale e longitudinale" - IST-01961 teso, appunto, alla rilevazione delle predette informazioni. In particolare l'Istat ha rappresentato l'intenzione di integrare tale lavoro, così come presente nel Psn 2014-2016, con il trattamento di dati personali, anche sensibili (origine razziale ed etnica, stato di salute) provenienti da trattamenti statistici di titolarità di soggetti rientranti nel Sistema statistico nazionale-Sistan (cd. soggetti Sistan) non presenti nel Psn (enti pubblici) nonché di enti "non Sistan" (associazioni).

Sul punto è stata rilevata la carenza, nella scheda identificativa del lavoro, di informazioni sufficienti all'Autorità per formulare il proprio parere. Infatti, lo stato ancora embrionale del progetto non consentiva all'Istat di evidenziare gli enti pubblici ovvero le associazioni presso i quali raccogliere i dati; il formato anonimo, aggregato (e in tal caso con che livello di aggregazione) ovvero individuale degli stessi e, nel caso di raccolta di dati personali non aggregati, le modalità previste per garantire la volontarietà dell'adesione alla ricerca da parte degli interessati. A causa delle genericità di tali elementi informativi, inoltre, la scheda informativa del lavoro statistico non risultava tale da costituire idonea informativa ai sensi dell'art. 13 del Codice e dell'art. 6, comma 2, del codice di deontologia. Su tali basi, per il trattamento di dati personali, anche sensibili, provenienti da trattamenti statistici, di titolarità di soggetti Sistan, non presenti nel Psn, nonché di enti non Sistan, l'Istat deve sottoporre al Garante, per l'acquisizione del parere di competenza, la relativa scheda identificativa IST-01961, opportunamente integrata e fornire preventivamente idonea informativa agli interessati (13 del Codice e dell'art. 6, comma 2, del codice di deontologia).

Il Garante ha così reso parere favorevole sul Programma statistico nazionale 2014-2016 Aggiornamento 2015-2016 con le indicazioni sopra riportate relative al lavoro statistico IST-01961 (prov. 18 settembre 2014, n. 411, doc. web n. 3458502).

Parere favorevole è stato espresso sui questionari da somministrare ai soggetti coinvolti nella sperimentazione della nuova *social card*, prevista dal d.l. 9 febbraio 2012, n. 5 (prov. 10 luglio 2014, n. 356, doc. web n. 3320745).

In particolare, l'art. 60, d.l. 9 febbraio 2012, n. 5, convertito con modificazioni in l. 4 aprile 2012, n. 35, recante "Disposizioni urgenti in materia di semplificazione e di sviluppo" prevede, nei comuni con più di 250.000 abitanti, l'avvio di una sperimentazione "al fine di favorire la diffusione della carta acquisti, istituita dall'articolo 81, comma 32, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, tra le fasce di popolazione in condizione di maggiore bisogno, anche al fine di valutarne la possibile generalizzazione come strumento di contrasto alla povertà assoluta", affidandone l'attuazione ad un decreto del Ministero del lavoro e delle politiche sociali (di seguito, Ministero) adottato di concerto con il Ministero dell'economia e delle finanze (Mef).

Su tale base normativa, il Ministero ha pertanto adottato il decreto del 10 gennaio 2013, recante disposizioni per l'attuazione della sperimentazione della nuova carta acquisti, che prevede in più fasi il coinvolgimento del Garante.

Tale decreto dispone, in particolare, che i Comuni destinatari della sperimentazione individuino due gruppi nell'ambito dei nuclei familiari beneficiari della *social*

Social card

card. Uno di tali gruppi è destinato a partecipare: i nuclei familiari appartenenti al primo gruppo partecipano ad un progetto personalizzato volto al superamento della condizione di povertà, al reinserimento lavorativo e all'inclusione sociale; i nuclei familiari appartenenti al secondo gruppo, invece, pur ricevendo la *social card*, non sono coinvolti nel predetto progetto personalizzato e costituiscono un gruppo di controllo. A tale ultimo gruppo è affiancato un ulteriore gruppo di controllo composto da non beneficiari della *social card* (artt. 1, comma 1, lett. *b*), *d*) e *g*) e 3, comma 1, lett. *c*) ed *f*) del decreto).

La sperimentazione della *social card* è oggetto di valutazione da parte del Ministero, di concerto con il Mef, da realizzarsi secondo quanto descritto in un apposito progetto di ricerca, redatto in conformità all'art. 3 del codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, All. A.4. al Codice (di seguito codice di deontologia). Tale valutazione intende principalmente accertare l'efficacia dell'integrazione del sussidio economico con i servizi a sostegno dell'inclusione attiva nel favorire il superamento della condizione di bisogno (art. 9 del decreto).

Per la realizzazione del progetto di ricerca in questione, i Comuni, designati responsabili del trattamento dal Ministero e dal Dipartimento del tesoro del Mef, collaborano somministrando questionari, predisposti dal Ministero "con l'assenso del Garante per la protezione dei dati personali", ai nuclei familiari beneficiari e al gruppo di controllo dei non beneficiari all'avvio e al termine della sperimentazione (art. 9 del decreto).

In tale quadro il Ministero ha quindi chiesto il previsto "assenso" del Garante sui questionari che intende somministrare "agli adulti ed ai bambini suddivisi in fasce di età 8-13 anni e 14-17 anni".

L'Autorità ha reso il parere di competenza su una versione dei questionari, predisposti nell'ambito del piano di valutazione elaborato dal Ministero di concerto con il Mef e con la collaborazione dell'Isfol, che tiene conto delle indicazioni e degli accorgimenti forniti dall'Ufficio ai competenti uffici del Ministero nel corso di numerosi incontri, anche informali, volti a garantire che le predette rilevazioni avvengano nel rispetto della disciplina in materia di protezione dei dati personali, con specifico riferimento alla tutela dei diritti fondamentali e alla dignità degli interessati coinvolti.

In tale ambito, il Ministero ha provveduto, in particolare, a collocare l'informativa (art. 13 del Codice e art. 6 del codice di deontologia) in posizione tale che gli interessati possano prenderne visione prima della sottoposizione alle domande che compongono i questionari. Il Ministero ha inoltre accolto il suggerimento dell'Ufficio di privilegiare, nella redazione dell'informativa, un registro piuttosto colloquiale, tale da risultare agevolmente comprensibile agli interessati. Inoltre, con specifico riferimento ai questionari, accanto ad ogni quesito dal quale è possibile desumere informazioni sensibili, è stato correttamente evidenziato che, in tali ipotesi, non sussiste obbligo di risposta, con ciò ribadendo quando già precisato nell'informativa (art. 9, comma 6, lett. *a*), del decreto).

In particolare, il Garante ha verificato che le informazioni raccolte con i questionari fossero pertinenti, non eccedenti e, con riferimento ai dati sensibili e giudiziari, indispensabili rispetto alle finalità che con essi si intende perseguire (artt. 11 e 22 del Codice e art. 9 del decreto).

9

I trattamenti da parte di Forze di polizia

9.1. *Il controllo sul Ced del Dipartimento della pubblica sicurezza*

A seguito delle 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 dell'art. 10, l. 1° aprile 1981, n. 121, come modificato dall'art. 175 del Codice.

9.2. *Altri interventi in relazione alle Forze di polizia*

Il Dipartimento della pubblica sicurezza del Ministero dell'interno ha chiesto al Garante di valutare un progetto sperimentale di ripresa visiva nel corso dello svolgimento di pubbliche manifestazioni, attraverso l'assegnazione a personale specificamente individuato di Reparti Mobili della Polizia di Stato di microtelecamere per l'eventuale ripresa di quanto avviene in situazioni di criticità per l'ordine pubblico.

Esaminato il progetto, il Garante ha rilevato che il trattamento di dati personali così effettuato appare finalizzato alla tutela dell'ordine e della sicurezza pubblica, la prevenzione, l'accertamento o la repressione dei reati e, quindi, sulla base delle disposizioni vigenti in materia di ordine pubblico, rientra nelle previsioni di cui all'articolo 53 del Codice, che esclude l'applicabilità a tali fattispecie di alcune disposizioni del Codice stesso (nota 31 luglio 2014, doc. web n. 3423775).

Il Garante, tuttavia, ha ricordato che anche i trattamenti di cui all'art. 53 del Codice debbono rispettare i principi di cui all'art. 11 del Codice medesimo, sicché i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

È stato pertanto indicato che il sistema di ripresa video sopra descritto dovrà essere attivato solo in caso di effettiva necessità, ossia di insorgenza di concrete e reali situazioni di pericolo di turbamento dell'ordine e della sicurezza pubblica. È pertanto opportuno che l'attività di formazione del personale di polizia destinato ad utilizzare i sistemi di ripresa – e, segnatamente, dei funzionari deputati a disporre l'attivazione e lo spegnimento – riguardi anche le regole concernenti la protezione dei dati personali; inoltre, in caso di effettuazione di riprese in occasione di situazioni di ritenuto pericolo per l'ordine e la sicurezza pubblica poi non concretizzatosi, venga disposta la tempestiva cancellazione delle immagini riprese in quanto il loro ulteriore trattamento risulterebbe estraneo alle finalità di cui all'art. 53 del Codice. Analogamente, è necessario che le immagini siano conservate per il solo tempo necessario al perseguimento delle finalità sottese al trattamento e che, al termine, esse siano cancellate. Dovranno inoltre essere designati gli incaricati del trattamento e adottate le misure di sicurezza di cui agli artt. 31 e ss. del Codice.

**Microtelecamere mobili
alle manifestazioni**

È stato espresso dal Garante parere favorevole (prov. 15 maggio 2014, n. 244, doc. web n. 3259425) sullo schema di Convenzione tra il Ministero dell'interno e i gestori di servizi di telecomunicazioni che regola l'accesso telematico delle Forze di polizia – previsto dalla legge e autorizzato solo per finalità di giustizia – a taluni dati riferiti ai detentori di telefoni fissi e mobili, tramite il Centro di elaborazione dati (Ced) del Dipartimento della pubblica sicurezza, utilizzando uno specifico sistema informatico denominato Elenco Telefonico Nazionale (E.T.Na.).

E.T.Na.

Gli approfondimenti al riguardo intercorsi su alcuni aspetti della Convenzione hanno consentito di introdurre maggiori garanzie per i possessori di telefoni fissi e mobili.

Il sistema consente la consultazione delle banche dati dei vari gestori e non comporta la creazione di un nuovo archivio né la duplicazione di informazioni. Tutti gli accessi ai dati saranno tracciati e potranno avvenire solo da postazioni di lavoro certificate; il personale che consulta il sistema dovrà essere in possesso di specifici profili di abilitazione e credenziali di autenticazione personali.

Il flusso di comunicazione dovrà essere protetto da elevati *standard* di sicurezza e non potranno essere utilizzati dispositivi automatici che consentono di consultare i dati in forma massiva.

Per i gestori tlc è stato tra l'altro introdotto l'obbligo di trasmettere al Ced un *report* delle attività di monitoraggio e controllo delle operazioni effettuate dal personale che utilizza E.T.Na.

Come anticipato (cfr. par. 3.4), il Garante ha espresso il proprio parere su uno schema di regolamento recante disposizioni di attuazione della legge 30 giugno 2009, n. 85 (di "ratifica" del "Trattato di Prüm" relativo alla cooperazione transfrontaliera per contrastare, in particolare, il terrorismo, la criminalità transfrontaliera e la migrazione illegale) per il funzionamento della Banca dati nazionale del dna e del relativo Laboratorio centrale, istituiti, rispettivamente, presso il Ministero dell'interno-Dipartimento della pubblica sicurezza e presso il Ministero della giustizia-Dipartimento dell'amministrazione penitenziaria.

**Banca dati nazionale
del dna**

La Banca dati è istituita "al fine di facilitare l'identificazione degli autori dei delitti" (art. 5, comma 1, l. n. 85/2009) e, a tal fine, provvede alla raccolta dei profili del dna di soggetti tassativamente indicati (sottoposti a custodia cautelare, a detenzione o a misura di sicurezza detentiva, per delitti, non colposi, per i quali sia consentito l'arresto facoltativo in flagranza, con esclusione di alcune fattispecie di reato), relativi a reperti biologici acquisiti nel corso di procedimenti penali, di persone scomparse o loro consanguinei, di cadaveri e resti cadaverici non identificati, consentendone il raffronto a fini di identificazione. Il Laboratorio centrale provvede, a sua volta, alla tipizzazione del profilo del dna dei soggetti e alla conservazione dei campioni biologici dai quali sono tipizzati i profili del dna. Il controllo sulla Banca dati è esercitato dal Garante nei modi previsti dalla legge.

Con il medesimo provvedimento l'Autorità ha espresso anche la prevista "intesa" con le amministrazioni interessate sui tempi per i quali i profili del dna restano inseriti nella Banca dati, che non possono essere superiori a 40 anni dall'ultima circostanza che ne ha determinato l'inserimento, e quelli di conservazione dei campioni biologici, che non possono superare i 20 anni (artt. 13, comma 4, e 16, l. n. 85/2009).

Lo schema di regolamento disciplina le modalità di trattamento e di accesso per via informatica e telematica ai dati raccolti nella Banca dati e nel Laboratorio, le modalità di comunicazione dei dati e delle informazioni richieste, le tecniche e le modalità di analisi e conservazione dei campioni biologici, nonché i tempi di conservazione dei campioni biologici e dei profili del dna nonché le modalità di cancellazione dei profili del dna e di distruzione dei relativi campioni biologici nei casi previsti.

Anche in considerazione dell'importanza della materia e della delicatezza dei trattamenti lo schema di regolamento è stato attentamente elaborato nell'ambito di un tavolo di lavoro istituito presso il Ministero dell'interno, cui ha partecipato, fin dalla sua costituzione, anche l'Ufficio.

Nel corso delle numerose riunioni, delle interlocuzioni e degli approfondimenti anche informali che ne sono seguiti, l'Autorità ha formulato rilievi e fornito indicazioni volte a rendere il testo conforme alla disciplina in materia di protezione dei dati personali. Le indicazioni hanno riguardato, in particolare, l'esigenza di individuare tempi di conservazione dei profili del dna e dei campioni biologici proporzionati rispetto alle finalità perseguite in linea con i criteri individuati dalla normativa europea (gravità del reato commesso, pericolosità del soggetto); di individuare altresì le operazioni di trattamento dei dati consentite al personale, specificamente abilitato e incaricato del trattamento dei dati personali, in servizio presso i laboratori delle Forze di polizia, il Laboratorio centrale e la stessa Banca dati, rispetto alle finalità in concreto perseguite e le relative modalità del trattamento; di definire le responsabilità sotto il profilo della protezione dei dati dei soggetti coinvolti, a vario titolo, nell'applicazione del regolamento, ovvero in relazione ai trattamenti di dati personali effettuati, rispettivamente, dai titolari, dai responsabili e dagli incaricati del trattamento; di pervenire ad una più chiara descrizione della configurazione della Banca dati sui previsti due livelli, sia rispetto ai dati raccolti in essi, sia in relazione alle finalità rispettivamente perseguibili mediante il loro trattamento, al fine di assicurarne la compatibilità, anche sotto il profilo tecnico, con il quadro normativo vigente, nazionale ed europeo; di addivenire ad un'adeguata regolamentazione degli aspetti di sicurezza dei sistemi e del trattamento dei dati personali, volta ad assicurare elevati *standard* di protezione, fisica e logica, delle informazioni raccolte nella banca dati e dei dati trattati per il funzionamento dei laboratori; di dettare una puntuale disciplina transitoria che regoli la confluenza nella banca dati dei profili del dna acquisiti nel corso di procedimenti penali anteriormente alla data di entrata in vigore della legge n. 85/2009, nei limiti di quanto consentito dal dettato normativo; di definire una puntuale disciplina degli scambi informativi con gli altri Paesi UE per finalità di cooperazione transfrontaliera in conformità a quanto disposto dalla normativa europea (Decisioni del Consiglio UE nn. 615 e 616 del 2008).

Parere favorevole è stato altresì espresso su uno schema di regolamento – proposto dal Ministro dell'Interno – volto a definire le modalità di funzionamento e collegamento della Banca nazionale unica della documentazione antimafia con il Ced interforze del Dipartimento della pubblica sicurezza ed altre banche dati, emanato in attuazione dell'art. 99, comma 1, d.lgs. 6 settembre 2011, n. 159 (cd. "codice antimafia"). L'archivio consentirà di semplificare il rilascio della documentazione antimafia sulle imprese (cd. "comunicazioni" e "informazioni" antimafia) alle stazioni appaltanti e agli altri soggetti legittimati ad acquisirle (pubbliche amministrazioni, camere di commercio, ordini professionali, ecc.). I dati registrati potranno essere trattati elettronicamente solo attraverso terminali attivati presso le Prefetture e presso gli altri soggetti legittimati all'accesso. Considerata la delicatezza e la mole dei dati, per interrogare l'archivio occorrerà utilizzare credenziali di autenticazione in base a specifici profili di autorizzazione. Tutti i dati saranno sottoposti a cifratura e verrà conservata la registrazione degli accessi. Le informazioni potranno essere trattate anche per finalità di applicazione delle normative antimafia oltre che dalle Prefetture anche da alcuni uffici del Dipartimento della pubblica sicurezza del Ministero dell'interno, dalle Forze di polizia, dalla struttura tecnica del Comitato di coordinamento per l'alta sorveglianza delle grandi opere e, nell'ambito delle attività di coordinamento del procuratore nazionale antimafia, dalla Direzione nazionale antimafia. Il parere dell'Autorità

**Banca nazionale unica
della documentazione
antimafia**

è stato reso su una versione dello schema già perfezionata in coerenza con le indicazioni suggerite dall'Ufficio, che hanno riguardato, in particolare, le finalità del trattamento dei dati, la specificazione delle banche dati collegate, una maggiore selettività degli accessi, l'obbligo di cancellazione dei dati alla scadenza dei termini di conservazione, la previsione espressa del conforme parere del Garante sulle convenzioni che dovranno disciplinare i collegamenti con alcuni sistemi informativi e l'aggiornamento da parte dell'impresa delle informazioni ad essa riferite presenti nella banca dati.

Sono stati chiesti chiarimenti da parte del Ministero dell'interno sull'utilizzo di droni, prospettandone l'ascrivibilità alla generale categoria della videosorveglianza (art. 2.2. lett. a), classe B, d.m. n. 269/2010), anche in relazione alle eventuali prescrizioni da emanare, con riferimento al regolamento di servizio necessario per l'utilizzo della tecnologia in parola.

Al riguardo, si è rilevato trattarsi di materia con implicazioni estese – poiché gli apparecchi possono essere usati per scopi assai diversi – e delicate, per i rischi specifici che possono derivarne per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati acquisibili ed alle modalità del trattamento.

In questo quadro, nel rappresentare che il tema è oggetto di analisi da parte dell'Autorità nell'ambito del Gruppo Art. 29 (cfr. par. 23.3), ci si è limitati per il momento a rappresentare che non sembrano automaticamente riferibili ai droni le determinazioni del Garante in materia di videosorveglianza.

In tal senso l'art. 22 del regolamento Enac sui mezzi aerei a pilotaggio remoto del 16 dicembre 2013, entrato in vigore il 30 aprile 2014, sottopone il trattamento di dati personali effettuato tramite gli strumenti in parola al rispetto del Codice, con particolare riguardo all'utilizzo di modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3 del Codice) nonché delle misure e degli accorgimenti a garanzia dell'interessato prescritti dal Garante.

Più dettagliate valutazioni in ordine ad ipotesi di utilizzo degli apparecchi potranno quindi essere formulate – alla luce delle valutazioni risultanti in ambito europeo – sia in esito ad una verifica preliminare, ai sensi dell'art. 17 del Codice, richiesta dagli operatori che vi abbiano interesse, sia nel fornire parere, ai sensi dell'art. 154, comma 4, del Codice, in ordine a schemi di atti di carattere generale volti a disciplinare la materia.

È pervenuto un quesito relativo alle modalità di raccolta dei dati personali da parte della Guardia di finanza nel corso dello svolgimento di una verifica fiscale presso uno studio legale. Al riguardo, si è rappresentato che, in termini generali, questa Autorità non ha tra i suoi compiti istituzionali la risposta a quesiti e, di regola, non fornisce riscontro ove essi siano posti da soggetti professionalmente chiamati ad interpretare le norme di legge e ad esprimersi sulla loro applicazione. Pertanto, salvo ogni apprezzamento dell'interessato in relazione al caso concreto, si è osservato che a dati trattati con l'ausilio di strumenti elettronici da organi uffici o comandi di polizia è applicabile l'art. 56 del Codice, che rinvia alle procedure disciplinate dall'art. 10, l. n. 121/1981.

9.3. *Il controllo sul sistema di informazione Schengen*

Il Ministero dell'interno-Dipartimento della pubblica sicurezza ha rappresentato l'opportunità di differire l'adempimento delle misure non ancora attuate tra quelle prescritte dal Garante volte a rafforzare la sicurezza nel trattamento dei dati effettuati per l'attuazione della Convenzione di Schengen, in ragione sia delle innova-

Droni

**Accertamenti disposti
dal Garante**

zioni 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 il provv. 31 luglio 2014, n. 391 (doc. web n. 3471761), ha disposto il differimento dei termini per l'adempimento delle prescrizioni, che sono in corso di attuazione.

Accesso diretto

Come è noto, 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 anche quest'anno 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.

10 L'attività giornalistica

Costante è stato l'impegno rivolto alla valutazione di segnalazioni e reclami concernenti casi di trattamenti di dati personali effettuati nell'esercizio dell'attività giornalistica. Come in passato, ciò è avvenuto, tenendo anche conto delle diverse modalità con cui si esercita l'attività di informazione, avendo come principale quadro di riferimento normativo il Codice (in particolare, gli artt. 136-139) e l'allegato codice di deontologia, in un'ottica di bilanciamento tra libertà di informazione e diritto alla riservatezza e alla protezione dei dati personali. In più casi, questo problema si è posto con riferimento ai dati personali di personaggi pubblici (uomini politici e appartenenti al mondo dello spettacolo), specie quando i loro dati sono stati acquisiti mediante artifici e raggiri (cfr. par. 10.3).

Un nuovo filone di provvedimenti del Garante è quello dei ricorsi che i cittadini hanno presentato contro Google nei casi di mancato accoglimento da parte della società di richieste di deindicizzazione di dati personali presentate in attuazione dei principi affermati in una recente sentenza della Corte di giustizia dell'Unione europea (cfr. par. 10.4) tenendo altresì contro dei criteri dettati dal Gruppo Art. 29 (v. WP 225, doc. web n. 3876849).

10.1. *I minori*

Con riferimento al rapporto tra libertà di informazione e tutela della riservatezza dei minori, il Garante è intervenuto nei confronti di alcune testate giornalistiche che, nel dar conto di vicende concernenti alcune studentesse minorenni hanno riportato dettagli eccedenti (idonei ad identificare le interessate) tratti da brani di intercettazioni e dalle dichiarazioni delle ragazze. Il Garante, da un lato, ha vietato alle testate di riportare i dati personali riferiti alle minorenni; dall'altro, ha richiamato i media e i gestori di siti web al più rigoroso rispetto dei principi a tutela dei minori sanciti dalla Carta di Treviso e dal codice deontologico dei giornalisti. In particolare, ha ribadito che il rispetto delle garanzie poste a tutela dei minori riguarda anche il dovere di astenersi dal pubblicare stralci di atti processuali la cui diffusione potrebbe pregiudicarne la dignità (provv. 14 luglio 2014, n. 351, doc. web n. 3267450).

Il Garante ha adottato un provvedimento nei confronti di You-tube chiedendo di rimuovere un video pubblicato dal "Movimento Pro Stamina Italia" nel quale veniva ripresa, in modo da poter essere identificata, una bambina di quattro anni gravemente malata, con indebita diffusione di dati personali sensibili (provv. 18 gennaio 2014, n. 23, doc. web n. 2923201).

10.2. *La cronaca giudiziaria*

Sono stati esaminati dal Garante segnalazioni e reclami relativi al trattamento di dati personali nell'ambito della cronaca giudiziaria; ciò sempre in un'ottica di bilanciamento tra la tutela della riservatezza e della dignità delle persone e esigenze di

Prostituzione minorile

Video Pro Stamina

Informazioni relative a procedimenti

informazione e trasparenza sull'attività di amministrazione della giustizia, in attuazione dei principi di finalità, non eccedenza e proporzionalità del trattamento dei dati (note 30 giugno e 15 luglio 2014).

Vittime di reato

Come in passato, l'Autorità ha ribadito che, nella diffusione di notizie relative a procedimenti penali, particolare cautela deve essere adottata al fine di assicurare il diritto alla riservatezza e il rispetto della dignità delle persone offese da un reato. Ciò in considerazione del fatto che la pubblicità data a tale offesa può costituire per l'interessato un'ulteriore violazione dei propri diritti.

10.3. *I personaggi pubblici e l'utilizzo di artifici e raggiri*

Affrontando il tema della raccolta e della diffusione di informazioni riguardanti personaggi pubblici o che esercitano pubbliche funzioni – per i quali la diffusione di informazioni, pur se relative alla sfera privata, può risultare giustificata in ragione della “qualificazione del protagonista” (art. 6, comma 1, del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica), ovvero considerato il rilievo sul ruolo o sulla vita pubblica del soggetto cui le informazioni si riferiscono (art. 6, comma 2), ovvero, ancora, quando le medesime siano tratte da dichiarazioni o comportamenti pubblici degli interessati (art. 137, comma 3, del Codice) – il Garante ha ritenuto che non potesse essere diffuso il video che ritraeva un esponente politico, ritratto insieme ad alcuni pazienti, durante la sua permanenza all'interno di una casa di cura nella quale stava spiando la pena comminatagli attraverso l'affidamento al servizio sociale. Ciò considerato che il giornalista si era introdotto nella casa di cura, luogo non aperto al pubblico, senza dichiarare la propria identità, e aveva raccolto le immagini dell'interessato e dei pazienti ivi ricoverati mediante una microcamera ai fini della successiva diffusione, violando in tal modo le disposizioni relative alla correttezza nella raccolta dei dati (prov. 10 luglio 2014, n. 352, doc. web n. 3373321).

In altra vicenda l'Autorità ha intimato di non diffondere (nell'ambito di un noto programma televisivo) interviste fatte ad alcuni dipendenti del Senato, riprese con telecamera nascosta, che avevano consapevolmente rilasciato dichiarazioni a persone qualificatesi come giornalisti (ignari però delle riprese video ed audio) (cfr. nota 30 luglio 2014).

L'Ufficio ha altresì richiesto l'adesione spontanea ai principi normativi richiamati in una nota facente seguito ad una opposizione relativa ad una trasmissione televisiva nella quale veniva intervistato un noto attore, il quale aveva lamentato che il giornalista gli aveva rivolto domande su temi diversi da quelli concordati riguardanti la propria attività teatrale, come quello delle abitazioni private, in particolare concentrandosi sul mancato pagamento di alcuni canoni di locazione relativi ad un appartamento, oggetto di un provvedimento di sfratto. In particolare, l'Ufficio ha ritenuto che il giornalista aveva violato il principio di correttezza nell'esercizio dell'attività giornalistica e ha ottenuto la cancellazione spontanea del menzionato video dal sito web (nota 4 agosto 2014).

Esaminando la segnalazione con la quale un esponente politico ha lamentato un trattamento illecito di dati personali in relazione alla registrazione e alla successiva diffusione (durante una trasmissione radiofonica) della conversazione telefonica fatta con una persona che, imitando la voce di un altro esponente politico, lo aveva tratto in inganno circa la reale identità dell'interlocutore telefonico, il Garante ha ribadito il principio per cui il giornalista non può utilizzare artifici e raggiri per raccogliere notizie che potrebbero essere acquisite con gli strumenti propri dell'inchiesta

giornalistica (provv. 11 settembre 2014, n. 400, doc. web n. 3405138). Al riguardo il Garante ha rilevato che le modalità di raccolta dei dati del segnalante sono risultate in violazione dell'obbligo, sussistente in capo a chi effettua trattamenti a fini giornalistici, di rendere note le finalità della raccolta e, in particolare, di evitare l'uso di "artifici" (art. 2, comma 1, del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica).

Infine, il Garante ha ritenuto eccedente la pubblicazione su un quotidiano dell'indirizzo e della fotografia aerea dell'abitazione di un noto conduttore televisivo e ne ha vietato la diffusione, anche in considerazione del potenziale pregiudizio alla sicurezza dell'intervistato e della propria famiglia (provv. 11 settembre 2014, n. 399, doc. web n. 3471605).

10.4. *Gli archivi storici e le informazioni online*

In materia di informazioni *online*, ha suscitato un acceso dibattito e determinato rilevanti conseguenze pratiche la menzionata sentenza 13 maggio 2014 nel caso Google Spain, con la quale la Corte di giustizia ha stabilito che il gestore di un motore di ricerca su internet è titolare del trattamento dei dati personali che appaiono su pagine web pubblicate da terzi. La decisione è rilevante anzitutto perché estende la nozione di stabilimento prevista dall'art. 4, par. 1, lett. *a*), della direttiva 95/46/CE, ricomprendendo tra i trattamenti effettuati "nel contesto delle attività di uno stabilimento del responsabile (ndr. titolare per il Codice) di tale trattamento nel territorio di uno Stato membro" anche quelli posti in essere, in uno Stato membro, da una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da un motore di ricerca la cui attività si dirige agli abitanti di detto Stato membro.

Secondo la Corte, inoltre, il gestore di un motore di ricerca è "obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei *link* verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi" (anche quando la loro pubblicazione sia di per sé lecita). Questo obbligo si manifesta nel caso di dati inesatti, ma anche nel caso in cui "essi siano inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento, [...] non siano aggiornati, oppure [...] siano conservati per un arco di tempo superiore a quello necessario, a meno che la loro conservazione non si imponga per motivi storici, statistici o scientifici".

A parere della Corte di giustizia, il diritto ad ottenere la cancellazione dei *link* al proprio nome prevale, "in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse [del] pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi".

È da evidenziare che l'ampia interpretazione fornita dalla Corte di giustizia alla nozione di stabilimento ha consentito di applicare la disciplina di protezione dei dati di matrice europea anche ai trattamenti effettuati dai "giganti della rete", a prescindere dalla questione dell'interpretazione della nozione di "strumento/*equipment*" prevista dall'art. 4, par. 1, lett. *c*), della direttiva. Attribuire però ai gestori dei