

rispetto delle disposizioni che il Codice prevede in questo ambito, in particolare per quanto riguarda l'acquisizione del consenso dell'interessato (cfr. artt. 76 e 85, comma 2, del Codice).

È stata poi evidenziata la necessità di integrare lo schema di decreto, prevedendo che anche ai sistemi di sorveglianza e ai registri, già disciplinati a livello nazionale, si applichino le cautele in materia di protezione dei dati personali individuate dal decreto, fatte salve le norme più restrittive eventualmente previste dalle specifiche discipline di settore, in quanto la normativa istitutiva di tali sistemi e registri è per lo più precedente al Codice.

L'intervento dell'Autorità ha, infine, consentito di introdurre l'obbligo per i titolari del trattamento dei dati, contenuti nei sistemi di sorveglianza e dei registri, di avvisare tempestivamente il Garante nel caso in cui queste informazioni subiscano violazioni (cd. *data breach*), al fine di scongiurare il rischio di accessi abusivi e di garantire l'esattezza e la continuità della fruibilità dei dati contenuti (si pensi a attacchi informatici, incendi o altre calamità, che possano comportare la perdita, la distruzione o la diffusione indebita di dati; cfr. artt. 4, comma 3, lett. g-bis e 32-bis del Codice). Ciò, in linea con le prescrizioni emanate dall'Autorità con riferimento alle grandi banche dati pubbliche e in considerazione del fatto che un'analoga previsione è contenuta nello schema di decreto per la disciplina del fascicolo sanitario elettronico (art. 24, comma 9), in relazione al quale il Garante ha reso a suo tempo parere (v. Relazione 2014, par. 6.1.2).

Sempre in tema di sistemi informativi centralizzati della sanità, il Garante ha espresso il proprio parere su un altro schema di decreto del Ministero della salute riguardante i requisiti di qualità e sicurezza del sangue e degli emocomponenti (prov. 25 giugno 2015, n. 379, doc. web n. 4172235). Lo schema disciplina tutti gli aspetti inerenti il percorso trasfusionale, dalla selezione del donatore fino all'infusione nel paziente, ivi compresa la donazione di cellule staminali emopoietiche, operando così la revisione dei decreti del 3 marzo 2005.

Al riguardo, l'Autorità ha, innanzitutto, rilevato che i decreti sopracitati del 2005 sono stati adottati senza il previo parere del Garante. In particolare, lo schema di decreto presenta implicazioni con il sistema informativo dei servizi trasfusionali (Sistra), che è stato istituito in virtù di un decreto, adottato il 21 dicembre 2007 senza il parere dell'Autorità. I sistemi informatici utilizzati nelle diverse strutture territoriali che concorrono all'attività trasfusionale alimentano questo sistema informativo centralizzato, che a sua volta raccoglie ed elabora flussi informativi relativi alle predette attività.

Riguardo alle modalità con cui i dati sulle attività trasfusionali sono memorizzati nel Sistra, l'Autorità ha segnalato la necessità di operare un'approfondita valutazione al fine di evitare il rischio di isolare e re-identificare i donatori e/o i pazienti, tenuto conto sia degli attributi prescelti per caratterizzare ciascun interessato (ad es., le iniziali del cognome e del nome) sia dell'esiguo numero di casi rilevati. Su tale aspetto, nel parere, è stata suggerita al Ministero la possibilità di impiegare, come "codice paziente" o come "codice donatore", un numero progressivo numerico o un codice *random*, per tutelare la riservatezza degli interessati, in ragione della delicatezza dei dati trattati (ad esempio nel caso di donatori risultati positivi ai test HIV, Hcv, Hbv e Treponema Pallidum).

Altre osservazioni hanno riguardato il modulo di informativa e di consenso al trattamento dei dati personali sia per i donatori di sangue e degli emocomponenti, sia per i donatori di sangue da cordone ombelicale. Sul punto, l'Autorità ha richiesto al Ministero di integrare il decreto, in relazione al caso in cui i dati personali dell'interessato siano trattati per finalità di ricerca scientifica, prevedendo che i servizi

Qualità e sicurezza
del sangue e
degli emocomponenti

trasfusionali raccolgano un autonomo e specifico consenso dell'interessato. A tal fine, va altresì predisposta un'informativa circostanziata che indichi, tra l'altro, anche per categorie, i soggetti destinatari dell'eventuale trasferimento del materiale donato e l'eventuale ambito di comunicazione dei dati, nonché gli elementi indicati nell'autorizzazione generale n. 8 laddove le attività volte a gestire la donazione possano comportare il trattamento di dati genetici (cfr. artt. 78, comma 5, lett. a), 90 e 105, comma 2, del Codice).

Inoltre, con riferimento al trasferimento di sangue da cordone ombelicale a scopo di ricerca scientifica ad altre banche della rete nazionale per la conservazione del sangue cordonale o ad altre strutture ospedaliere del Ssn, è stato suggerito di prevedere che tale trasferimento possa essere effettuato a condizione che il materiale biologico venga irreversibilmente anonimizzato per garantire la riservatezza degli interessati.

Sotto il profilo della sicurezza dei dati, il Garante, ha evidenziato, infine, la necessità di assicurare l'accesso selettivo alle informazioni conservate nei sistemi gestionali informatici dei servizi trasfusionali e il loro utilizzo proporzionato rispetto alle finalità perseguite, nonché di migliorare le previsioni del decreto relative alla registrazione delle operazioni di accesso (*log*) alla cifratura e alla separazione dei dati anagrafici dai dati sanitari e genetici.

Trapianto di organi

Il Garante è stato chiamato ad esprimersi sulla delicata materia dei trapianti di organi, con il parere reso su uno schema di decreto del Ministero della salute recante attuazione della direttiva 2010/53/UE, relativa alle norme di qualità e sicurezza degli organi umani destinati ai trapianti, nonché della direttiva 2012/25/UE sullo scambio tra Stati membri di tali organi (prov. 28 maggio 2015, n. 315, doc. web n. 4168076).

Il decreto fa riferimento a tutte le fasi del processo di donazione e trapianto dell'organo, cioè alla donazione, all'analisi, alla caratterizzazione, al reperimento, alla conservazione, al trasporto, al trapianto e alla fase di eliminazione di organi prelevati. Altri aspetti rilevanti della materia e, in particolare, le modalità di funzionamento del Sistema informativo trapianti, le modalità di generazione del numero identificativo nazionale del donatore e del ricevente e i necessari trattamenti di dati sensibili saranno invece oggetto di un successivo provvedimento dell'Amministrazione, avente natura regolamentare, in relazione al quale l'Autorità ha assicurato la più ampia collaborazione in vista dell'espressione del parere di competenza. Il Garante ha ritenuto, di dover mettere in luce la necessità che la definizione delle modalità di composizione del numero identificativo nazionale del donatore e del ricevente tenga in adeguata considerazione l'esigenza di mantenere riservata l'identità degli interessati, ma allo stesso tempo assicuri la tracciabilità degli organi e quindi la possibilità di re-identificare questi ultimi qualora si ritenga necessario per salvaguardare la loro salute, suggerendo, in particolare, l'adozione di un sistema di identificazione indiretta.

Sotto il profilo della sicurezza dei dati, l'Autorità ha disposto di integrare lo schema di decreto con un disciplinare tecnico nel quale siano descritte misure e accorgimenti più incisivi al fine di proteggere i dati personali dei donatori e dei riceventi. Più in generale, è stata raccomandata l'adozione da parte dei centri trapianti, delle strutture ospedaliere e degli altri enti coinvolti nella donazione di organi, di una rigorosa politica di sicurezza delle informazioni che tenga anche in considerazione l'esigenza di garantire la qualità, la disponibilità e la non disconoscibilità degli stessi dati.

Lo schema di decreto ha previsto, inoltre, la possibilità che, attraverso il Centro nazionale trapianti, il Ministero della salute possa stipulare accordi con Paesi terzi o

organizzazioni europee per lo scambio di organi con la specifica previsione di misure tecniche e di sicurezza relative alla trasmissione delle informazioni. Nel merito, il Garante ha avvertito la necessità che tale previsione tenga in dovuta considerazione l'art. 44 del Codice in tema di trasferimento di dati verso Paesi non appartenenti allo spazio economico europeo, poiché, in virtù di tali accordi, non può escludersi che lo scambio di organi comporti il trasferimento di dati personali riferiti al donatore o al ricevente.

L'attività consultiva obbligatoria del Garante ha riguardato, infine, uno schema di decreto del Ministero della salute volto a disciplinare lo *screening* neonatale esteso (sne) per la diagnosi di patologie metaboliche ereditarie (prov. 2 aprile 2015, n. 196, doc. web n. 3943315). Al riguardo, è stata sottolineata la delicatezza della materia regolata dal decreto che consente il trattamento di dati sanitari e, nei casi in cui lo sne sia positivo, di informazioni riguardanti la possibilità che il neonato sviluppi in futuro determinate malattie generiche che, peraltro, devono essere comunicare al Registro nazionale delle malattie rare di cui al d.m. 18 maggio 2001, n. 279.

Il Garante si è espresso favorevolmente sullo schema di decreto, auspicando tuttavia un intervento migliorativo dell'articolato, con particolare riferimento alla previsione della raccolta del consenso al trattamento dei dati sanitari e genetici, unitamente al consenso informato all'atto medico, previa idonea informativa (art. 13 del Codice e punto 5 dell'autorizzazione generale n. 8).

Nell'informativa dovrà essere evidenziato, in particolare, il carattere facoltativo (ovvero obbligatorio, nelle regioni che lo hanno previsto) del conferimento dei dati per lo sne, le specifiche finalità perseguite (segnatamente cura e, qualora lo sne dia esito positivo, consulenza genetica), i risultati conseguibili anche in relazione ad eventuali notizie inattese che possono essere conosciute per effetto dell'effettuazione dello sne, l'ambito di comunicazione dei dati, specie con riferimento a quella verso il Registro nazionale delle malattie rare. Con l'occasione, è stata inoltre segnalata l'opportunità che il modello di informativa possa includere anche il trattamento dei dati finalizzato allo *screening* neonatale obbligatorio disciplinato dal d.P.C.M. 9 luglio 1999.

Le indicazioni dell'Autorità hanno riguardato, poi, le misure di sicurezza con particolare riferimento alla conservazione separata dei dati personali sulla salute dagli altri dati personali, all'adozione di protocolli operativi per il trasporto dei campioni che garantiscono la custodia e la tracciabilità degli stessi, alla previsione di accorgimenti idonei a proteggere le informazioni relative ai casi positivi allo sne.

Infine, è stata richiamata l'attenzione dell'amministrazione sull'opportunità che le iniziative di aggiornamento professionale, previste dal decreto, siano focalizzate anche sulla materia della protezione dei dati personali.

Screening neonatale

6 I dati genetici

Cessione a terzi
di una banca dati
genetica della
popolazione sarda

L'Autorità a seguito del fallimento di una società di ricerca aveva avviato lo scorso anno alcuni accertamenti in merito alla destinazione di una banca dati genetica della popolazione sarda, contenente i campioni biologici di circa dodici mila individui insieme ai dati demografici, clinici, genetici e genealogici riguardanti rapporti di parentela risalenti fino al 1600 (cfr. Relazione 2014, p. 71). Sulla base delle informazioni e dei documenti acquisiti presso il curatore fallimentare, in merito alle attività prodromiche all'eventuale cessione a terzi della banca dati, l'Ufficio ha raccomandato il rispetto della disciplina sulla protezione dei dati personali nei casi di cessazione del trattamento, con particolare riferimento all'osservanza del principio di finalità e delle altre disposizioni il cui mancato rispetto determinerebbe l'inefficacia dell'atto di trasferimento e l'inutilizzabilità dei dati trasferiti (v. artt. 11, 16 e 162, comma 1, del Codice).

Sotto questo profilo, è stato suggerito di predisporre l'avviso per l'acquisizione delle manifestazioni di interesse in modo da assicurare che il potenziale acquirente fornisca idonee garanzie circa gli scopi di ricerca scientifica, avendo cura che tali finalità siano perseguite direttamente dal nuovo titolare del trattamento e risultino quindi coerenti con l'oggetto dell'attività principale svolta da quest'ultimo (cfr. art. 28 del Codice e, sia pure con riferimento a una fattispecie di altro tenore, Relazione 2005, pp. 65-66). Riguardo agli altri presupposti di liceità del trasferimento della banca dati, è stata sottolineata la necessità di fornire agli interessati un'idonea informativa e di acquisire il consenso con riferimento al complesso dei trattamenti di dati che la cessione comporta, ivi compreso l'eventuale trasferimento all'estero della banca dati, in modo da garantire in concreto a ciascun interessato la possibilità di esercitare il controllo sui dati e sui campioni che lo riguardano (artt. 13, 26 e 43, comma 1, lett. a) e 90 del Codice). Ciò, fatta salva la possibilità di richiedere all'Autorità un'autorizzazione *ad hoc*, ai sensi dell'art. 90 del Codice, qualora a causa di particolari ragioni non sia possibile informare gli interessati malgrado sia stato compiuto ogni ragionevole sforzo per raggiungerli (v. punto n. 8.1, autorizzazione generale n. 8/2014 e provv. 11 dicembre 2014, n. 590, doc. web n. 3632835).

Inoltre, considerata l'estrema delicatezza dell'ingente patrimonio genetico della popolazione sarda racchiuso nella banca dati, è stato raccomandato di incrementare il livello di sicurezza dei dati e dei campioni attualmente conservati, mediante l'adozione delle misure tecnico-organizzative previste dalla citata autorizzazione generale n. 8., ponendo particolare attenzione al controllo degli accessi ai locali della società in liquidazione, ai sistemi di autenticazione informatica per la consultazione della banca dati, nonché alle tecniche di cifratura o all'utilizzo di codici identificativi volti a ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato alla banca dati (nota 15 giugno 2015).

Nel corso dell'anno è stato affrontato il tema delle biobanche e dei campioni biologici a fini di ricerca.

Un caso ha riguardato la legge della Regione Sicilia 1° ottobre 2015, n. 22 recante "Istituzione delle biobanche di ricerca in Sicilia" sulla quale l'Autorità ha fornito alla Presidenza del Consiglio dei ministri elementi di valutazione per l'even-

Biobanche a fini
di ricerca

tuale impugnazione davanti alla Corte costituzionale ai sensi dell'art. 127 della Costituzione (cfr. par. 3.5).

L'Autorità ha evidenziato al riguardo che, seppure non esista in materia una legge nazionale organica, il legislatore nazionale ha riservato una particolare attenzione al trattamento dei dati genetici apprestando un regime differenziato di regole e garanzie fissato con la citata autorizzazione generale n. 8 la quale ha, tra l'altro, tassativamente individuato le finalità di trattamento tra le quali, gli scopi di "ricerca scientifica e statistica finalizzati alla tutela della salute dell'interessato, di terzi o della collettività in campo medico, biomedico ed epidemiologico" (punto 3.1, lett. c).

È stata, in particolare segnalata l'indeterminatezza dell'art. 1, comma 1 della menzionata legge regionale, che dispone l'istituzione di biobanche di ricerca per la raccolta, la lavorazione, la conservazione, lo stoccaggio e la distribuzione di materiale biologico umano ad enti e gruppi di ricerca regionali, nazionali e internazionali, senza indicare le specifiche finalità che possono giustificare il trattamento delle informazioni sanitarie e genetiche associate a tale materiale. È stata quindi evidenziata la non conformità della norma all'art. 117, comma 1, Cost. che sancisce che la potestà legislativa delle regioni deve essere esercitata "nel rispetto dei vincoli derivanti dall'ordinamento comunitario", tra i quali devono annoverarsi anche quelli in materia di protezione dei dati personali e, in particolare, il principio di finalità (cfr. art. 6.1a) direttiva 95/46/CE e art. 11 del Codice). Inoltre, è stato rilevato che la citata disposizione presenta profili di incompatibilità anche con l'art. 117, comma 2, lett. d) della Costituzione, in quanto la regione, nel regolamentare il trattamento dei dati genetici in contrasto con i principi e le regole sulla protezione dei dati, stabiliti a livello nazionale, ha invaso una competenza legislativa riservata esclusivamente allo Stato che rientra nella materia dell'ordinamento civile (cfr. Corte costituzionale, sentenza n. 271/2005).

Criticità di analogo tenore sono state sollevate con riferimento alle disposizioni sulle fonti del materiale biologico delle biobanche che prevedono di utilizzare, tra l'altro, materiale diverso da quello specificamente prelevato e conservato per uso di ricerca, senza operare alcun richiamo ai presupposti e ai previsti limiti legislativi (si pensi al materiale biologico residuo derivato da interventi diagnostici o terapeutici o a quello risultato non idoneo al trapianto). Com'è noto, l'autorizzazione generale sul trattamento dei dati genetici prevede come regola generale, la raccolta del consenso dell'interessato, salvo talune tassative eccezioni (punto 3. c) e 8.1 dell'autorizzazione generale n. 8 (v. al riguardo anche raccomandazione (2006)4 del Consiglio d'Europa sull'utilizzo di campioni biologici di origine umana per scopi di ricerca, art. 12) (nota 19 novembre 2015).

La recente legge della Regione Sicilia 21 gennaio 2016, n. 2 ha modificato la menzionata legge 1° ottobre 2015, n. 22 recependo — nella sostanza — le indicazioni fornite dal Garante. Sempre sul tema delle biobanche di ricerca è stata avviata una collaborazione con l'Istituto nazionale dei tumori che ha richiesto all'Ufficio, un approfondimento su un progetto di istituzione e regolamentazione di una biobanca di campioni biologici a scopo di ricerca in campo oncologico, nell'intendimento di giungere a soluzioni condivise, rispettose delle esigenze della protezione dei dati personali e genetici degli interessati. Sono stati esaminati diversi profili tra i quali la delimitazione delle finalità di ricerca perseguite, l'individuazione delle categorie di soggetti da cui viene prelevato il materiale biologico, gli elementi essenziali dell'informativa e del consenso (comprese le conseguenze di un'eventuale revoca dello stesso), le modalità di raccolta e di utilizzo dei dati sanitari e genetici associati al materiale biologico, le cautele per consentire l'accesso da parte di ricer-

Servizi personalizzati
di prevenzione medico-
genetica online

catori interni e esterni, i requisiti dei progetti di ricerca nonché le misure tecniche e organizzative per garantire la sicurezza dei dati e dei campioni contenuti nella biobanca, con particolare riferimento al prospettato sistema di codificazione dei dati.

In relazione a un quesito formulato da una società che intendeva offrire *online* un servizio personalizzato a pagamento di prevenzione medico-genetica, l'Ufficio ha avuto modo di precisare che le finalità del trattamento dei dati necessari all'erogazione del servizio sono riconducibili a quelle di tutela della salute dell'interessato previste dalla citata autorizzazione generale n. 8, piuttosto che a quelle di ricerca scientifica in ambito medico. È stato però rilevato che le prospettate modalità di registrazione *online* degli utenti per l'attivazione del servizio e la raccolta del campione biologico non sono risultate idonee ad accertare univocamente l'identità del soggetto al quale viene effettuato il prelievo, come richiede invece la predetta autorizzazione (v. punto 4) (nota del 27 aprile 2015).

7

La ricerca scientifica e la statistica

7.1. La ricerca scientifica

Nel 2015 si è reso necessario evidenziare a università, enti di ricerca e società scientifiche che la possibilità di trattare dati sulla salute per scopi di ricerca scientifica in campo medico, biomedico ed epidemiologico, a prescindere dal consenso delle persone coinvolte nello studio, è un'ipotesi residuale prevista dal Codice, nell'eventualità in cui il titolare del trattamento si trovi in presenza di particolari e comprovate circostanze dalle quali derivi l'impossibilità di informare gli interessati e lo studio sia oggetto del parere favorevole del competente comitato etico a livello territoriale (artt. 106, 107 e 110 del Codice e autorizzazione generale n. 9 al trattamento dei dati personali effettuato per scopi di ricerca scientifica, n. 591, doc. web n. 3632879).

In tale quadro, è stato precisato che non è possibile rilasciare autorizzazioni *ad hoc* ai sensi degli artt. 41 e 110 del Codice, senza allegare all'istanza di autorizzazione il parere del comitato etico, ovvero senza evidenziare i profili del trattamento dei dati che si intende effettuare in difformità alle prescrizioni della predetta autorizzazione generale n. 9, nonché in assenza di documentazione idonea a comprovare le situazioni eccezionali non considerate nella predetta autorizzazione che giustificerebbero l'accoglimento della richiesta (note 6 maggio e 3 luglio 2015).

All'Ufficio è stato poi richiesto di fornire le proprie indicazioni in merito al progetto di una Regione volto a realizzare un osservatorio regionale sul fenomeno della violenza contro le donne. Il progetto prevedeva in particolare, la creazione, all'interno di una banca dati regionale informatizzata, dei cd. fascicoli (elettronici) donna, a cura dei centri antiviolenza e delle case rifugio del territorio, contenenti dati personali, anche sensibili e giudiziari, riguardanti il percorso di ciascuna donna vittima di violenza presa in carico. Il progetto prevedeva altresì che l'accesso alle informazioni, elaborate in forma aggregata, era consentito anche alla Regione per svolgere attività di monitoraggio del fenomeno. È stato chiarito al riguardo che l'attività di monitoraggio del fenomeno della violenza contro le donne di competenza regionale, può essere utilmente svolta mediante il trattamento di soli dati anonimi.

Al contrario, le misure di anonimizzazione dei dati prospettate, consistenti nella cancellazione dell'intera componente anagrafica, sono state ritenute insufficienti in quanto non idonee ad eliminare la possibilità di isolare l'insieme dei dati riferiti alla singola vittima, rendendo quest'ultima re-identificabile (art. 4, comma 1, lett. n), del Codice; v. anche Gruppo Art. 29, parere n. 5/2014 sulle tecniche di anonimizzazione – WP 216).

Ulteriori perplessità sono state manifestate riguardo alla validità del consenso della vittima, come presupposto legittimante la creazione dei predetti fascicoli elettronici, considerate le situazioni di estrema vulnerabilità delle donne esposte a minacce (o vittime) di maltrattamenti e di violenze di ogni genere le quali potrebbero temere di non ricevere assistenza e sostegno adeguati, qualora non acconsentissero al trattamento di dati in questione (cfr. art. 23, comma 4, del Codice e Gruppo Art. 29, parere n. 15/2011 sulla definizione di consenso - WP 187).

Inoltre, la raccolta in un unico fascicolo elettronico dei dati delle vittime e la loro condivisione tra gli enti del territorio coinvolti non sono state ritenute indispensa-

Osservatorio regionale
antiviolenza

Piano d'azione straordinario contro la violenza di genere

Trasferimento all'estero di dati di farmacovigilanza

Censimento della popolazione, delle abitazioni e dei numeri civici delle strade urbane (Annctu)

bili per fornire l'assistenza necessaria alle donne interessate. Ciò, tenuto conto anche degli specifici limiti che la disciplina prevede per le operazioni di raffronto e per i trattamenti volti a definire il profilo e la personalità dell'interessato utilizzando banche dati di diversi titolari (art. 22, comma 11, del Codice) (note 6 ottobre e 19 novembre 2015).

Sotto altri profili, sono in corso alcuni approfondimenti sulla conformità alla normativa sulla protezione dei dati personali delle modalità di attuazione del Piano d'azione straordinario contro la violenza sessuale e di genere di cui all'art. 5, d.l. 14 agosto 2013, n. 93, conv. in l. 15 ottobre 2013, n. 119. In particolare, il Piano prevede la creazione di un sistema informativo nazionale integrato di raccolta ed elaborazione dei dati sulla violenza contro le donne provenienti da una molteplicità di fonti (amministrative in ambito sanitario, giuridico sociale e del terzo settore).

Al riguardo, l'Ufficio ha manifestato la propria disponibilità a collaborare con il Dipartimento per le pari opportunità della Presidenza del Consiglio dei ministri e con le altre amministrazioni interessate, al fine di identificare adeguate garanzie in relazione ai profili di competenza in materia di protezione dei dati personali (nota 6 ottobre 2015).

In risposta a una società farmaceutica, che aveva richiesto l'autorizzazione per la migrazione dei dati sulla farmacovigilanza in un nuovo *database*, situato in Svizzera, sotto il controllo della capogruppo francese, l'Ufficio ha rappresentato che per il trasferimento di queste informazioni in Paesi non appartenenti allo spazio economico europeo non è necessario ottenere una specifica autorizzazione, se il trattamento è effettuato in presenza di uno dei presupposti indicati nell'art. 44 del Codice (prov. 13 maggio 2015, n. 290, doc. web n. 4167370).

In particolare, per effettuare la migrazione dei predetti dati sulla farmacovigilanza (ovvero informazioni sulle reazioni avverse a medicinali non direttamente identificative dei pazienti nonché dati identificativi dei segnalatori quali medici, altri operatori sanitari o gli stessi pazienti), la società intendeva avvalersi della collaborazione di alcuni fornitori di servizi stabiliti in Svizzera e di un'altra società con sede in India.

Al riguardo, è stato precisato che la società farmaceutica avrebbe potuto trasferire questi dati alla società avente sede in India, a condizione di designare quest'ultima quale responsabile del trattamento ai sensi dell'art. 29 del Codice e di stipulare con la medesima le clausole contrattuali di cui all'allegato della decisione 2010/87/UE, 5 febbraio 2010 della Commissione europea (cfr. autorizzazione 27 maggio 2010, n. 35, doc. web n. 1728496). Non sono stati ravvisati poi ostacoli al trasferimento verso i fornitori di servizi stabiliti in Svizzera (sempre che questi siano designati responsabili del trattamento), poiché l'ordinamento di tale Paese offre un livello adeguato di protezione dei dati personali (cfr. decisione della Commissione 2000/518/CE 26 luglio 2000 e autorizzazione del Garante 17 ottobre 2001, doc. web n. 39428).

Con l'occasione, è stata infine segnalata l'opportunità di adottare tecniche di codificazione adeguate per la memorizzazione dei dati sanitari riguardanti le reazioni avverse ai medicinali (cfr. art. 3 del Codice e Titolo IX d.lgs. 24 aprile 2006, n. 219).

7.2. La statistica

Il Garante ha formulato il parere sullo schema di d.P.C.M. in materia di censimento della popolazione e delle abitazioni e dell'Archivio nazionale dei numeri civici delle strade urbane (Annctu) (prov. 15 ottobre 2015, n. 536, doc. web n. 4481301).

Lo schema di decreto è risultato parzialmente coerente rispetto ad alcune delle

indicazioni fornite nell'ambito di incontri di lavoro preliminari tenutisi con i rappresentanti dell'Istat e della Presidenza del Consiglio dei ministri, mentre ha mostrato profili di criticità nella parte riguardante il nuovo censimento della popolazione residente da effettuarsi con cadenza annuale (cd. censimento permanente).

Nello specifico, tenuto conto che le disposizioni concernenti l'istituzione e il funzionamento dell'Annscu non prevedono espressamente la raccolta di dati personali per la realizzazione del predetto Archivio, l'Autorità non ha formulato alcun rilievo. Tuttavia, poiché le previste interconnessioni con altre banche dati possono comportare trarramenti di dati personali, ha condizionato il parere favorevole all'espressa previsione che sul provvedimento interdirigenziale dell'Istat e dell'Agenzia delle entrate — da adottarsi per la definizione delle specifiche tecniche e delle modalità di accesso ai servizi dell'Annscu — sia acquisito un ulteriore parere del Garante.

Con riferimento, invece, al censimento permanente, è stata rilevata l'inidoneità del decreto a disciplinare le modalità e l'organizzazione del censimento poiché tale atto deve stabilire unicamente i tempi di realizzazione.

Diversamente, alcuni articoli dello schema intervengono invece a disciplinarne fonti, modalità di realizzazione, flussi di dati che invece necessitano di un corretto inquadramento giuridico.

In particolare, oltre a stabilire la tempistica di un primo ciclo di indagini campionarie per il 2021, viene introdotta una nuova modalità di realizzazione del censimento permanente, prevedendo, in carenza di idonei presupposti normativi, l'integrazione di "fonti diverse relative a individui, famiglie, abitazioni ed edifici con i risultati di indagini campionarie, volte a valutare gli errori di copertura dell'anagrafe e a soddisfare le esigenze informative statistiche". Al riguardo l'Autorità ha evidenziato che la raccolta di dati personali da parte dell'Istat con obbligo di risposta e le operazioni di sperimentazione del censimento permanente attraverso atti di pianificazione tecnico-organizzativa possono avvenire soltanto se previste dal Programma statistico nazionale-Psn ovvero da norme di legge o regolamento.

Sono stati censurati inoltre alcuni aspetti volti ad introdurre nuovi flussi di dati non "definitivi" e quindi protetti dal segreto statistico verso soggetti facenti parte del Sistan e, verso non meglio qualificati organismi di rilevazione, in assenza di qualsiasi garanzia per gli interessati.

Analoghe osservazioni critiche sono state effettuate in relazione all'abbassamento della soglia di diffusione dei dati risultanti dal censimento permanente, anche con frequenza inferiore alle tre unità. Sul punto l'Autorità ha ribadito che una tale disposizione può essere contenuta unicamente in un atto normativo idoneo (in questo caso norma di legge o Psn), come peraltro avvenuto in passato.

L'Autorità ha, inoltre richiamato con forza l'attenzione delle amministrazioni competenti sulla circostanza che, come per il precedente 15° censimento generale della popolazione, alcuni aspetti del censimento trovino disciplina in un atto avente forza di legge che, anche attraverso il rinvio a successivi atti amministrativi o in parte al Psn, ne stabilisca le modalità di realizzazione.

Sotto altro profilo, il Garante ha, invece, preso favorevolmente atto che lo schema di decreto è stato, in parte, modificato in conformità alle indicazioni fornite nel corso dei predetti incontri, volte ad assicurare, in particolare, il rispetto dell'art. 105 del Codice il quale prevede che i dati raccolti per fini statistici non possano essere utilizzati per prendere decisioni o provvedimenti nei confronti dell'interessato, né per trattamenti di dati per scopi di altra natura.

Il Garante, con parere 29 ottobre 2015, n. 566 si è espresso sullo schema di Programma statistico nazionale (Psn) 2014-2016 – Aggiornamento 2016 (doc. web n. 4476104).

Programma statistico
nazionale (Psn)

Il parere ha riguardato i trattamenti di dati personali inseriti nel Psn e le modifiche ai prospetti identificativi relativi a lavori statistici che comportano il trattamento di dati personali già inclusi nel Psn 2014-2016 e nel relativo Aggiornamento 2015-16, sui quali il Garante aveva espresso il parere con i provvedimenti 26 giugno, n. 324 e 18 settembre 2014, n. 411 (doc. web nn. 3320710 e 3458502).

In via preliminare, l'Autorità ha rilevato il costante aumento dell'impiego da parte dell'Istat dei sistemi informativi che, duplicando intere banche dati amministrative e statistiche, raccolgono e conservano informazioni personali relative alla totalità dei cittadini, o rilevanti gruppi di individui. Attraverso l'utilizzo di dati amministrativi e fonti statistiche in tali sistemi vengono, infatti, ricostruite le connessioni logiche esistenti fra le singole unità, sfruttando i codici d'identificazione univoci delle persone fisiche (codice fiscale) censite nelle diverse banche dati (individui e famiglie con relative caratteristiche socio-demografiche, economiche, occupazionali e di istruzione ecc.), arrivando così a profilare l'intera cittadinanza in relazione ad ogni aspetto della vita quotidiana in prospettiva diacronica, ivi compresa la relativa posizione geografica.

Il Garante ha rilevato, altresì, che i sistemi informativi prevedono la conservazione delle informazioni in "forma personale", corredate degli identificativi diretti e che la costituzione di un sistema informativo rappresenta una delle ipotesi in cui è consentita la conservazione di dati identificativi anche oltre il periodo necessario per il raggiungimento degli scopi per i quali sono stati raccolti o successivamente trattati (cfr. art. 11 del codice di deontologia; pareri 24 settembre 2009, 10 giugno 2010 e 19 giugno 2014 rispettivamente doc. web nn. 1657731, 1734415 e 3320710).

Nello specifico, il Garante ha esaminato, in primo luogo, le caratteristiche del Sistema integrato dei microdati – IST-02270 Sistema di integrazione logico-fisica di microdati amministrativi e statistici (Sim), inserito per la prima volta nel Psn 2011-2013 come registro statistico nazionale degli individui. Si tratta di un sistema informativo in cui, nel corso degli anni, l'Istat ha fatto confluire circa 60 archivi di fonte amministrativa, per circa 500 milioni di *record* all'anno e che l'Istituto vorrebbe ampliare aggiungendo ulteriori banche dati. Nel Sim vengono quindi concentrati dati inerenti ad ogni aspetto della vita degli interessati, profilati attraverso tecniche di *linkage* e di georeferenziazione degli indirizzi, utilizzando luoghi di dimora abituali e domicilio, unità frequentate come luogo di lavoro, di studio, di abitazione e di cura, legami tra individui, luoghi, enti e istituzioni e anche le informazioni che saranno contenute nell'istituendo Anncsi.

Il Garante ha quindi evidenziato che nel Sim vengono conservati i dati identificativi diretti degli interessati, che non vengono cancellati dopo la raccolta.

Il Sim, infatti, viene utilizzato dall'Istat quale archivio intermedio per la realizzazione di numerosi altri lavori statistici (tra i quali rilevano, in particolare, altri sistemi informativi, i cd. *repository* e il censimento permanente), poiché permette di selezionare campioni ragionati, disponendo di unità campionarie già ampiamente corredate di informazioni personali.

Al riguardo, pur riconoscendo l'attitudine del Sim a ridurre i costi e il fastidio statistico, ha rilevato come la conservazione degli identificativi diretti attraverso nuove acquisizioni di dati da fonti amministrative e statistiche, determina la schedatura permanente di ogni individuo nel tempo e nello spazio, conducendo ad un costante incremento delle informazioni disponibili e all'esponenziale aumento del rischio di re-identificazione degli interessati in relazione a dati in principio aggregati o anonimi (ad es., i *big data*, cfr. anche il parere 05/2014 sulle tecniche di anonimizzazione del Gruppo Art. 29).

Il Garante si è, infine, soffermato sulla base integrata di microdati statistici per

L'analisi dell'occupazione IST-02264, basata sull'integrazione di archivi amministrativi e statistici di tipo LEED (*Linked Employer Employee Database*) contenente informazioni sulle imprese (datore di lavoro) e i lavoratori, ricavate da 18 basi dati amministrative e statistiche, è destinata ad essere integrata con l'acquisizione dell'archivio Uniemens dell'Inps relativa anche a dati sulla salute e a dati giudiziari. L'Autorità ha al riguardo rilevato l'impossibilità per l'Istat di conservare gli identificativi diretti degli interessati separatamente dagli altri dati personali nonostante, come più volte ribadito dal Garante, il Codice dispone "che i dati sensibili e giudiziari contenuti in elenchi, registri e banche dati siano 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 siano conservati separatamente da altri dati personali che non richiedono il loro utilizzo (art. 22, commi 6 e 7, del Codice)" (parere 26 giugno 2014, cit.).

Considerati gli evidenti rischi che le descritte modalità di utilizzo dei sistemi informativi statistici possono comportare per la tutela dei diritti e delle libertà fondamentali degli interessati il Garante ha ritenuto necessario che tali trattamenti siano sottoposti ad una verifica preliminare dell'Autorità per individuare adeguate garanzie volte ad assicurare l'applicazione dei principi in materia di protezione dei dati personali attraverso idonee misure ed accorgimenti (art. 17 del Codice).

Il Garante ha, poi, rilevato una grave criticità concernente l'utilizzo a fini amministrativi di dati trattati per finalità statistiche, riferibile sia alla vigilanza dell'Istituto sulla qualità della tenuta dei registri anagrafici che alla correzione dell'anagrafe da parte dei comuni (attività riconducibile a finalità amministrative non di competenza dell'Istat o di altri soggetti Sistan) e ha ribadito che i lavori contenuti nel Psn devono essere effettuati in conformità a quanto stabilito dal richiamato art. 105 del Codice.

Un aspetto di particolare rilievo ha riguardato inoltre lo studio progettuale quale attività di sperimentazione a supporto della Protezione civile per aggiornare e migliorare le mappe di rischio relative all'intero territorio nazionale e gli scenari per la valutazione della popolazione esposta. Considerata, infatti, l'insufficienza dell'utilizzo delle sole fonti censuarie e amministrative in specifici ambiti territoriali a rischio sismico, l'Istat intenderebbe utilizzare i *call detail record* (di seguito cdr), un sottoinsieme di informazioni che si generano durante un generico evento di chiamata da telefonia mobile, registrato dai vari gestori telefonici nei propri *server* per ciascuna utenza.

Al riguardo, tenuto conto delle rilevanti criticità che un siffatto trattamento può comportare in termini di protezione dei dati personali, l'Autorità ha ribadito quando evidenziato nel citato parere sul Psn – Aggiornamento 2015-2016 in relazione al lavoro IST-02589, *Uso a fini statistici dei big data*. Ciò, sia con riferimento al trattamento dei dati di traffico relativi alla telefonia mobile (cdr), ancorché raccolti in forma anonima presso il gestore telefonico, che ai connessi rischi di reidentificazione degli interessati, soprattutto in caso di eventuali confronti con *set* di microdati dell'Istituto.

L'Autorità ha ritenuto necessario che l'Istat sottoponga preventivamente al Garante la metodologia da adottare in tale studio al fine di integrare opportunamente il prospetto identificativo IST-02645 per l'acquisizione del relativo parere.

In merito alla prevista possibilità di rilasciare microdati a soggetti Sistan e consentire l'accesso agli stessi da parte di ricercatori nell'ambito di specifici laboratori di analisi dei dati, l'Autorità, ha richiamato quanto rilevato nell'ambito dell'apposito tavolo tecnico avviato con l'Istat in materia di diffusione e scambio di microdati raccolti in ambito Sistan circa il necessario quadro di garanzie da introdurre per tali trattamenti di dati ed in particolare, conformemente a quanto previsto sul punto dal

regolamento (UE) n. 557/2013/UE della Commissione 17 giugno 2013 relativo all'accesso a dati riservati destinati a fini scientifici, ha evidenziato la necessità che:

- sussistano specifici requisiti per l'ente di ricerca di appartenenza dei ricercatori e per il progetto di ricerca per le cui finalità vengono richiesti i dati;
- i *file* di dati elementari, privi di ogni riferimento che permetta l'identificazione diretta delle unità statistiche, siano predisposti dal soggetto Sistan che ne concede l'accesso, tenendo conto dei tipi di dati nonché dei rischi e delle conseguenze di una loro illecita divulgazione;
- siano vietati trattamenti diversi da quelli esplicitamente previsti dal progetto di ricerca, la conservazione dei dati elementari oltre i termini di durata dello stesso, la comunicazione ulteriore dei dati a terzi, nonché la diffusione;
- le modalità di organizzazione e funzionamento dei laboratori fisici e virtuali che consentono l'accesso ai dati assicurino che i risultati della ricerca non permettano il collegamento con gli interessati e, comunque, secondo modalità che rendano questi non identificabili anche indirettamente.

In sede istruttoria è emerso che l'Istat non ha ancora completato la predisposizione del questionario da somministrare nell'ambito del lavoro statistico IST-02660 Metodologia e organizzazione della rilevazione della popolazione residente in altro tipo di alloggio all'interno di campi autorizzati e tollerati, che prevede il trattamento di dati idonei a rivelare l'origine razziale ed etnica degli interessati.

Il Garante ha, pertanto, ritenuto necessario che l'Istituto, prima dell'avvio della rilevazione, trasmetta all'Autorità, per le necessarie valutazioni di competenza, copia dell'informativa e del questionario.

8

I trattamenti da parte di Forze 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, l. 1° aprile 1981, n. 121, come modificato dall'art. 175 del Codice.

8.2. Altri interventi riguardanti le Forze di polizia

Nel 2015 sono giunte diverse segnalazioni relative all'installazione di sistemi di videosorveglianza nelle case circondariali, nelle quali si lamentava, tra l'altro, il mancato rispetto delle procedure previste dall'art. 4 dello Statuto dei lavoratori (l. n. 300/1970), con riferimento alla possibilità che tali sistemi riprendessero anche l'attività del personale di Polizia penitenziaria. Il Garante ha rilevato che il rapporto di lavoro del personale di Polizia penitenziaria è sottratto all'applicazione della disciplina dettata in materia di pubblico impiego con il d.lgs. 30 marzo 2001, n. 165, il cui art. 42 prevede che "nelle pubbliche amministrazioni la libertà e l'attività sindacale sono tutelate nelle forme previste dalle disposizioni della legge 20 maggio 1970, n. 300". Pertanto per l'applicazione dello Statuto al rapporto di lavoro degli agenti di polizia penitenziaria occorre fare riferimento all'art. 37 dello Statuto stesso, in base al quale "le disposizioni della presente legge si applicano altresì ai rapporti di impiego dei dipendenti dagli enti pubblici, salvo che la materia sia diversamente regolata da norme speciali". Secondo la giurisprudenza amministrativa una disposizione dello Statuto dei lavoratori si applica al dipendente di un ente pubblico (non soggetto alla disciplina di cui al cit. d.lgs. n. 165/2001) "solo nel caso in cui manchi del tutto la disciplina relativa al caso di specie nell'ambito dell'ordinamento interno dell'ente stesso" (C.d.S., n. 708/1990, n. 95/1995, Tar Liguria n. 415/2006). Ebbene, nell'ordinamento interno del Corpo di polizia penitenziaria sussistono norme specifiche che riguardano l'applicazione di nuove tecnologie e misure volte a migliorare la sicurezza degli istituti penitenziari con effetti generali sull'organizzazione del lavoro, nonché le relative forme di partecipazione sindacale, in funzione di tutela dei diritti e degli interessi dei lavoratori penitenziari coinvolti. In particolare, l'art. 19, comma 14, l. 15 dicembre 1990, n. 395, recante l'Ordinamento del Corpo di polizia penitenziaria, prevede che siano disciplinate con d.P.R., previa deliberazione del Consiglio dei ministri, sulla base di accordi stipulati da una delegazione composta dal Ministro per la funzione pubblica, che la presiede, dal Ministro della giustizia e dal Ministro del tesoro o dai Sottosegretari di Stato rispettivamente delegati, e i rappresentanti delle organizzazioni sindacali nazionali maggiormente rappresentative del personale, tra le altre, le "misure volte a migliorare l'efficienza e la sicurezza degli istituti". A sua volta, l'art. 26, comma 3, d.P.R. 18 giugno 2002, n. 164, nel recepire l'accordo sindacale per le Forze di polizia ad ordi-

Videosorveglianza
nelle carceri

8

namento civile e lo schema di concertazione per le Forze di polizia ad ordinamento militare relativi al quadriennio normativo 2002-2005 ed al biennio economico 2002-2003, stabilisce che “per il Corpo di polizia penitenziaria, l’amministrazione, per tutte le materie indicate negli articoli 25 e 27, procede, prima di assumere le relative determinazioni, all’esame previsto nel comma 1, nel rispetto dei termini massimi ivi stabiliti, dopo aver fornito alle organizzazioni sindacali firmatarie dell’accordo sindacale recepito con il presente decreto operanti presso il Corpo di polizia penitenziaria le informazioni necessarie”. Da tali disposizioni, aventi un ambito di applicazione assai ampio, emerge una disciplina speciale, rispetto a quella dell’art. 4 della l. n. 300/1970, per quanto riguarda l’uso di impianti audiovisivi e delle altre apparecchiature idonee al controllo a distanza dell’attività dei lavoratori, che risulta sottoposto non a contrattazione, ma, per quanto riguarda la Polizia penitenziaria, alla procedura in parola (v., in particolare, artt. 25 comma 4, lett. c) e 27, comma 1, lett. c).

Sussiste, pertanto, una specifica disciplina in tema di tecnologie finalizzate a garantire la sicurezza e la incolumità dei dipendenti e degli stessi detenuti che prevede la consultazione sindacale in luogo della più complessa procedura prevista dall’art. 4 dello Statuto dei lavoratori (accordo sindacale o, in mancanza, autorizzazione dell’ispettorato del lavoro) in ragione della natura dell’ambiente carcerario. Si è rilevato quindi che le procedure alternative di consultazione collettiva di cui al cit. d.P.R., non si pongono – in mancanza di esplicita previsione sull’inefficacia delle determinazioni assunte in violazione delle procedure stesse come condizione necessaria per il trattamento dei dati personali in parola, ma per disciplinare profili attinenti alle relazioni sindacali (nota 10 dicembre 2015).

Il Ministero dell’interno ha chiesto un parere in merito alla sperimentazione di microcamere da applicare sulla divisa degli operatori che espletano attività di controllo del territorio, poiché la registrazione visiva può costituire efficace strumento di prevenzione a tutela sia delle persone che del regolare svolgimento delle funzioni istituzionalmente attribuite al personale della Polizia di Stato.

Il Garante ha rilevato che, essendo tale sperimentazione finalizzata alla tutela dell’ordine e della sicurezza pubblica, alla prevenzione, accertamento e repressione dei reati, il trattamento rientra nella previsione di cui all’art. 53, comma 1, del Codice, sicché ad esso non si applicano le disposizioni indicate nel medesimo comma purché sia previsto in taluna delle fonti richiamate dal cit. art. 53, comma 2, come modificato dal d.l. n. 7/2015, convertito con l. 17 aprile 2015, n. 43. Il trattamento è, comunque, soggetto ad una valutazione di proporzionalità (art. 11 del Codice) ed è stata pertanto, indicata la riduzione dell’impiego del sistema in argomento ad alcuni casi specifici e predefiniti, espressione dei poteri, anche coercitivi, tipici delle Forze di polizia (ad es., effettuazione di un arresto). L’Autorità ha anche raccomandato cautele e limiti nella determinazione dei casi e tempi di conservazione delle immagini riprese, nonché dei termini di consultazione delle immagini nella puntuale designazione degli incaricati e, ove opportuno, dei responsabili, ai sensi e nei modi di cui agli artt. 29 e 30 del Codice. Ha inoltre richiesto che i sistemi informatici traccino ogni trattamento delle registrazioni, in modo che possa risalirsi univocamente al soggetto che ha effettuato l’accesso ed alla data ed ora in cui il trattamento è stato effettuato (nota 24 aprile 2015).

È stata segnalata al Garante la possibile violazione dei dati personali degli agenti di polizia coinvolti in riprese video di conferenze stampa relative alla divulgazione delle attività di polizia, ovvero di operazioni di polizia – talvolta simulate a titolo di esemplificazione – al fine della realizzazione di servizi giornalistici diffusi da telegiornali nazionali. L’Autorità ha rilevato che il caso in oggetto rientra nella disciplina

Sperimentazione
di microcamere

Videoriprese per
servizi giornalistici

di cui al Titolo XII (Giornalismo ed espressione letteraria ed artistica) del Codice, artt. 136-139, nonché nelle previsioni del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (riportato nell'All. A1 del Codice). Tale disciplina consente la diffusione degli altrui dati personali, anche senza il consenso dell'interessato, purché nei limiti del diritto di cronaca "e, in particolare, quello dell'essenzialità dell'informazione rispetto a fatti di interesse pubblico" (art. 137, comma 3, del Codice). L'articolo 6 del codice deontologico stabilisce che le notizie che assumano le caratteristiche del "rilevante interesse pubblico o sociale" possono essere divulgate, "quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti". Orbene, le conferenze stampa attraverso le quali si rende edotta l'opinione pubblica di rilevanti operazioni di polizia condotte dalle Forze dell'ordine appaiono senz'altro rientranti nel diritto di cronaca, come pure l'illustrazione alla cittadinanza delle iniziative assunte per garantire la sicurezza della navigazione durante i periodi estivi, come nel caso *de quo*. Le immagini delle persone coinvolte in tali contesti non sono diffuse illecitamente se, anche in associazione a eventuali commenti, non risultino lesive della dignità, identità e riservatezza delle persone ritratte (cfr. provv. 15 novembre 2012, n. 344, doc. web n. 2185342). Né è richiesto, nei casi di cui sopra, il consenso degli interessati (art. 137 del Codice). Peraltro, il Ministero dell'interno potrà, comunque, valutare l'opportunità di coinvolgere soggetti consenzienti, ancorché non sussista alcun obbligo al riguardo, come sopra precisato (nota 16 aprile 2015).

È pervenuto a questa Autorità un reclamo, da parte di una doganalista, in cui si lamentava che nel processo verbale di revisione delle dichiarazioni doganali, redatto dal competente ufficio territoriale e notificato ad alcune società importatrici, erano state riportate, al fine di fare valere la responsabilità solidale della segnalante con le società importatrici, informazioni sulla sua posizione di indagata in un procedimento penale ed in particolare sulle specifiche attività di indagine cui era stato sottoposta (atti di perquisizione e sequestro) e sulle risultanze delle indagini stesse.

Il Garante ha ritenuto la comunicazione a terzi di dati giudiziari della reclamante in contrasto con la disciplina rilevante in materia di dati personali, in materia di proporzionalità, (art. 11), di comunicazioni da parte di soggetti pubblici (art. 19), e di trattamento di dati giudiziari (art. 21, che richiama l'art. 20, comma 2). Più in dettaglio, la comunicazione di dati giudiziari della reclamante da parte dell'Agenzia delle entrate a terzi, al fine di consentire loro la conoscenza della responsabilità solidale dell'interessato per il pagamento di una sanzione amministrativa pecuniaria, non è prevista né consentita da alcuna norma di legge o di regolamento né è stata oggetto di parere del Garante. La presunta sussistenza del cennato vincolo di responsabilità solidale, ove ritenuta sussistente dall'Agenzia, poteva essere comunicata alle imprese importatrici interessate senza necessità di comunicare i dati giudiziari in argomento, per di più relativi ad un giudizio penale non concluso, onde da questo non poteva trarsi alcun argomento decisivo in ordine a profili di responsabilità, ancora oggetto di accertamento da parte del giudice penale (nota 24 aprile 2015).

Questa Autorità ha ricevuto una segnalazione da parte del Garante delle persone sottoposte a misure restrittive della libertà personale, secondo cui in una casa circondariale, a seguito della morte di una detenuta per assunzione di una *overdose* di sostanze stupefacenti, erano state effettuate analisi cliniche su tutte le altre detenute per verificare l'uso di tali sostanze ed i risultati, con l'indicazione del nome della persona cui si riferivano, erano stati trasmessi dalla locale Asl alla direzione del carcere, che li aveva utilizzati per comminare sanzioni disciplinari.

8

Dati giudiziari
nel verbale di revisione
delle dichiarazioni
doganali

Dati sensibili
delle detenute di
una casa circondariale

5

8

Questa Autorità, ha pertanto proceduto ad accertare il rispetto dei diritti delle detenute da parte dei soggetti pubblici che avevano effettuato gli accertamenti biologici nei loro confronti. Sulla base dei documenti prodotti e delle dichiarazioni fornite dalle amministrazioni coinvolte, è risultato che il prelievo delle urine delle detenute e le successive analisi cliniche era stato effettuato per lo svolgimento di attività di polizia giudiziaria (indagini relative allo spaccio delle sostanze stupefacenti "tagliate" male), di cui agli artt. 47 e ss. del Codice, e che le persone assoggettate al prelievo, informate in ordine allo scopo dello stesso, avevano fornito il loro consenso. Tuttavia, dalla documentazione si evinceva che le detenute erano state informate unicamente delle finalità del prelievo attinenti ad attività di polizia giudiziaria e non già della utilizzabilità dei risultati del medesimo al fine di comminare sanzioni disciplinari da parte dell'Amministrazione carceraria.

Orbene, l'art. 13 del Codice, applicabile ai trattamenti effettuati sia da soggetti pubblici che privati, stabilisce l'obbligo di fornire all'interessato una informativa, orale o scritta, in ordine alle caratteristiche del trattamento, compresa l'indicazione della natura obbligatoria o facoltativa del conferimento dei propri dati e le conseguenze di un eventuale rifiuto di rispondere. Nella specie si trattava di dati sensibili, ossia di dati idonei a rivelare lo stato di salute dell'interessato (art. 4, comma 1, lett. d). Le fonti normative che prevedono l'irrogazione di sanzioni disciplinari a carico delle persone detenute (l. 26 luglio 1975, n. 354, recante Norme sull'ordinamento penitenziario e sulla esecuzione delle misure privative e limitative della libertà, artt. 38 e ss. e d.P.R. 30 giugno 2000, n. 230, Regolamento recante norme sull'ordinamento penitenziario e sulle misure privative e limitative della libertà, artt. 77 e ss.) non specificano i tipi di dati sensibili e le operazioni di trattamento eseguibili nell'ambito dei procedimenti disciplinari. Il regolamento di cui al d.m. giustizia 12 dicembre 2006, n. 306 (recante la disciplina del trattamento dei dati sensibili e giudiziari da parte del Ministero della giustizia, adottato ai sensi degli artt. 20 e 21 del Codice) prevede (all. n. 8) il trattamento dei dati sensibili nell'ambito delle procedure e sanzioni disciplinari unicamente in riferimento alla "gestione del personale". Il trattamento dei dati sensibili dei detenuti è invece previsto, senza menzione di sanzioni disciplinari, nell'ambito dell'attività di assistenza sanitaria nei confronti dei soggetti detenuti (all. n. 10).

Pertanto il Garante ha ritenuto l'utilizzo, a fini disciplinari dei dati sensibili in parola non conforme alla disciplina relativa al trattamento dei dati personali, sia in quanto non era stata fornita alle persone interessate alcuna informativa al riguardo, come prescrive l'art. 13 del Codice, sia per la mancata previsione di tale tipo di trattamento di dati sensibili nelle fonti di riferimento, ai sensi di quanto prescrive l'art. 20, comma 2, del Codice e sia perché neppure risulta agli atti l'autorizzazione dell'autorità giudiziaria, ai sensi degli artt. 116 e ss. c.p.p., da considerare con riferimento all'art. 11 del Codice (prov. 1° ottobre 2015, n. 507, doc. web n. 4429647).

Un'altra segnalazione ha evidenziato che, presso una casa circondariale, durante le ore di chiusura della segreteria, le comunicazioni per malattia del personale erano ricevute telefonicamente dal personale della portineria, presso il quale veniva temporaneamente depositato l'apposito registro per l'annotazione delle assenze; il personale di portineria, tuttavia, non era stato nominato incaricato del trattamento dei dati personali dei lavoratori dell'istituto, come prescrive l'art. 30 del Codice.

L'Amministrazione carceraria ha ritenuto non necessaria la nomina degli addetti alla portineria ad incaricati del trattamento, sostenendo che la comunicazione, da parte di un dipendente, di non prendere servizio "per inalore" non integra la nozione di trattamento di un dato. Il Garante ha ritenuto, invece, che detta comunicazione riguarda dati personali, ai sensi dell'art. 4, comma 1, lettere b) e, in alcuni

Comunicazioni
delle assenze
per malattia in
una casa circondariale