SENATO DELLA REPUBBLICA

XVII LEGISLATURA

Doc. **CXXXVI**
n. **4**

RELAZIONE

SULL'ATTIVITA' SVOLTA DAL GARANTE E SULLO STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(ANNO 2015)

(Articolo 154, comma 1,lettera m), del codice di cui al decreto legislativo 30 giugno 2003, n. 196)

Presentata dal garante per la protezione dei dati personali
(SORO)

Comunicata alla Presidenza il 6 luglio 2016

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione2015

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 696773785
e-mail: garante@gpdp.it
www.garanteprivacy.it


Provvedimenti collegiali 692
307
Ricorsi decisi
44
Pareri resi al Governo
4.991
Riscontri dell'Autorità a segnalazioni e reclami
57
Provvedimenti su segnalazioni e reclami
27
Verifiche preliminari
€ 3.345.515
Sanzioni pagate
I numeri del 2015
2.622
Notificazioni pervenute
303
Ispezioni
1.696
Sanzioni contestate
33
Comunicazioni all'autorità giudiziaria
25.528
Risposte a quesiti
47
Comunicati e newsletter
5.023.069
Accessi al sito web

In evidenza – 2015

Gennaio

Su richiesta del Corpo nazionale soccorso alpino e speleologico, abbiamo ritenuto legittimo l'utilizzo di sistemi di geolocalizzazione idonei ad individuare lo *smartphone* di persone disperse in montagna, a condizione che i dati raccolti riguardino esclusivamente la posizione geografica dei terminali e che vengano utilizzati soltanto per salvaguardare la vita o l'integrità fisica degli infortunati [par. 11.9]

Abbiamo vietato ad una Regione l'ulteriore diffusione sul sito web istituzionale di dati idonei a rivelare lo stato di salute dei partecipanti ad una pubblica iniziativa riservata ai disabili e contestualmente ordinato la rimozione della copia web dagli indici e dalla *cache* dei motori di ricerca [par. 4.3]

Abbiamo dichiarato illeciti i trattamenti effettuati da un consorzio di polizia locale a mezzo di sistemi di videosorveglianza (all'interno delle autovetture di servizio) e di localizzazione dei palmari in dotazione ai dipendenti e vietato il trattamento di localizzazione (idoneo a consentire a tutti gli operatori di accedere ad una pluralità di dati dei colleghi) in quanto eccedente e non necessario al raggiungimento delle finalità perseguite nonché privo delle garanzie previste dallo Statuto dei lavoratori [par. 12.1]

Febbraio

Abbiamo dichiarato illecito e vietato l'ulteriore trattamento dei dati personali riferiti alla navigazione internet dei dipendenti di una società di comunicazione commerciale. Il monitoraggio del traffico in rete – idoneo a consentire al datore di lavoro di risalire all'identità dell'utilizzatore della singola macchina - veniva effettuato in assenza di una informativa e di una *policy* volta a disciplinare l'utilizzo degli strumenti elettronici da parte dei lavoratori [parr. 12.2 e 21.4]

In occasione della visita di una delegazione dell'Autorità per la protezione dei dati albanese è stato sottoscritto un Accordo di cooperazione tra le due autorità anche allo scopo di promuovere ispezioni congiunte sull'attività di *telemarketing* svolte dai *call center* [parr. 11.2 e 22.5]

È stato reso parere favorevole sullo schema di decreto del Direttore dell'Agenzia delle entrate che definisce le modalità tecniche per l'accesso alla dichiarazione 730 precompilata da parte del contribuente o di altri soggetti autorizzati (caf, sostituti di imposta e professionisti delegati) e che tiene conto delle indicazioni fornite dall'Autorità volte ad evitare accessi abusivi ai dati dei contribuenti [parr. 4.6 e 21.2]

Marzo

Abbiamo avviato una consultazione pubblica sul cd. *Internet of Things* (IoT) volta ad acquisire osservazioni e proposte riguardo ai profili di protezione dati connessi all'impiego di tecniche che consentono l'interazione e l'interconnessione di oggetti e sistemi diversi, allo scopo di fornire indicazioni per consentire agli utenti un reale controllo sui propri dati [par. 10.3]

Abbiamo subordinato il parere favorevole ad uno schema di regolamento del Ministero della salute sulle procedure per l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Ssn ad alcune specifiche integrazioni, quali la definizione di maggiori garanzie a tutela degli assistiti in relazione al sistema informativo delle schede di dimissione ospedaliera, alle modalità di accesso ai dati del Nsis e alle misure di sicurezza [parr. 3.4.1 e 5.2.1]

Allo scopo di armonizzare e semplificare le attività di profilazione *online* e garantire

maggiori tutele per gli utenti, abbiamo individuato in apposite Linee guida le regole che i fornitori dei servizi *online* devono rispettare (in particolare l'obbligatorietà del consenso informato dell'utente – sia autenticato che non autenticato e revocabile in qualsiasi momento – e dell'informativa) [par. 10.2]

Abbiamo vietato ad una Regione di diffondere ulteriormente i dati personali (valutazioni sulla professionalità di un dipendente alla base di un trasferimento) contenuti in una delibera pubblicata nell'albo pretorio *online* oltre il termine previsto dalla legge [par. 12.4]

Aprile

Abbiamo reso parere favorevole su uno schema di decreto concernente lo "*screening* neonatale esteso" (sne) ai fini della diagnosi precoce di patologie metaboliche ereditarie chiedendo alcune integrazioni riguardo al consenso informato dei genitori del neonato, all'informativa (che dovrà evidenziare il carattere facoltativo o obbligatorio del conferimento dei dati, le finalità di cura e di consulenza genetica, l'ambito di comunicazione dei dati). Il modello di consenso dovrà contenere l'eventuale dichiarazione di volontà dei genitori di conoscere i risultati dello *screening* [parr. 3.4.1 e 5.2.1]

Abbiamo reso parere favorevole su uno schema di decreto legislativo per il recepimento della direttiva 2013/37/UE del 26 giugno 2013, relativo al riutilizzo dell'informazione del settore pubblico che ha accolto, in fase di predisposizione, le indicazioni fornite dal Garante in merito al riutilizzo dei documenti i cui diritti di proprietà intellettuale sono detenuti da biblioteche, musei e archivi; ai limiti sull'accesso ai documenti che contengono dati personali che non sono conoscibili da chiunque; all'uso di licenze aperte disponibili *online* [parr. 2.1.2 e 3.4.2]

Maggio

Abbiamo prescritto a Sky Italia s.r.l. di vincolare all'inserimento di un codice individuale la possibilità di accedere al messaggio relativo alla richiesta di pagamento di rate insolute, inviato al *decoder* del cliente sotto forma di *banner* contenente l'icona di una busta, ritenendo altrimenti tale modalità comunicativa in grado di esporre il cliente al rischio di illecita diffusione di informazioni relative alla propria posizione debitoria [par. 13.7]

Abbiamo reso parere favorevole ad uno schema di decreto del Miur che regola la realizzazione e consegna di una carta nominativa dello studente denominata "IoStudio" che consente ai titolari di usufruire di agevolazioni per l'accesso a beni e servizi culturali e, a richiesta, di attivarla come carta di debito anonima al portatore. Il Garante ha accertato che vengano impiegati – e cancellati al termine dell'iniziativa – solo i dati indispensabili e che gli studenti ricevano l'informativa al momento dell'iscrizione *online* al primo anno della scuola secondaria [parr. 3.4.1 e 4.5]

Abbiamo condizionato il parere favorevole su uno schema di decreto del Mef concernente le regole tecnico-operative per il funzionamento del processo tributario telematico ad alcune precisazioni, soprattutto in merito alle modalità di identificazione dei soggetti legittimati ad accedere al Sistema informativo della giustizia tributaria, alle registrazioni delle operazioni di accesso al fascicolo informatico nonché alle acquisizioni dei *file* e degli atti nel registro generale [par. 3.4.1]

In occasione dello *Sweep day* 2015, dedicato alla protezione in rete dei ragazzi tra gli 8 e i 13 anni, abbiamo riscontrato (tra le *app* e i siti analizzati) rilevanti profili di criticità inerenti soprattutto alla trasparenza sulla raccolta e utilizzo di dati personali, alle autorizzazioni richieste, alla pubblicità e al rischio che i bambini vengano indirizzati verso siti non controllati [par. 22.5]

Giugno

Abbiamo adottato le nuove Linee guida in materia di *dossier* sanitario elettronico, allo scopo di fornire un quadro di riferimento unitario per il corretto trattamento dei dati e di garantire ai pazienti maggiori tutele ed elevati *standard* di sicurezza. È stato in particolare prescritto al titolare del trattamento l'obbligo di comunicare al Garante le violazioni dei dati (*data breach*), nonché riconosciuto al paziente il diritto alla visione degli accessi effettuati al proprio *dossier* sanitario [par. 5.1.2]

Abbiamo reso parere favorevole su uno schema di Linee di guida relative alla facoltà di annotare sulla carta d'identità il consenso o il diniego alla donazione di organi o tessuti in caso di morte. Le indicazioni fornite dal Garante - sull'informativa all'interessato, sulla possibilità di modificare in qualsiasi momento la manifestazione di volontà riportata sulla c.i., sui diritti riconosciuti dal Codice e sulle modalità di trasmissione dei dati tra comune e Sistema informativo trapianti (Sit) – sono state accolte [parr. 3.4.1 e 4.4]

Abbiamo autorizzato la Banca d'Italia, anche nel rispetto dell'autorizzazione n. 7/2014, al trattamento dei dati giudiziari dei collaboratori esterni che, in ragione della proprie mansioni, accedono a specifiche aree considerate "sensibili" sotto il profilo della sicurezza, al fine di consentire la preventiva verifica dei precedenti penali e dei carichi pendenti [par. 4.1]

Abbiamo chiesto maggiori garanzie a tutela della riservatezza delle lavoratrici nel parere espresso su uno schema di decreto interministeriale (elaborato dal Ministero del lavoro e delle politiche sociali) sulle modalità tecniche per la predisposizione e l'invio all'Inps dei certificati medici di gravidanza, interruzione della gravidanza e parto, con particolare riferimento all'invio telematico dei certificati su richiesta della lavoratrice, alle idonee misure di sicurezza e ai dati contenuti nei certificati [parr. 3.4.1 e 5.2]

Abbiamo ordinato ad una società, in qualità di datore di lavoro, di interrompere con effetto immediato il trattamento dei dati personali relativi alle conversazioni Skype tra una dipendente e soggetti terzi, in contrasto con le disposizioni ordinamentali a tutela della segretezza delle comunicazioni, le Linee guida del Garante del 2007 e la *policy* aziendale [par. 19.3]

Abbiamo reso parere su due provvedimenti dell'AgID: uno schema di regolamento in tema di modalità attuative per la realizzazione dello Spid (il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese) e un altro recante le relative regole tecniche. Sul medesimo tema siamo intervenuti nel corso dell'anno anche con riguardo alla procedura di rilascio dell'identità digitale da parte dei gestori accreditati e alle previste convenzioni fra l'AgID e i soggetti interessati. In tutti i casi, pur risultando i testi conformi alla gran parte delle osservazioni formulate dall'Autorità nell'ambito di un tavolo tecnico appositamente istituito, abbiamo chiesto ulteriori specificazioni a tutela degli interessati, come quella di perfezionare i livelli di sicurezza delle identità digitali [parr. 3.4.1. e 4.2]

Luglio

Abbiamo prescritto alle pp.aa. regole rigorose per l'interconnessione delle banche dati e l'obbligo di comunicare al Garante, entro quarantotto ore dalla conoscenza del fatto, le violazioni dei dati o gli incidenti informatici (cd. *data breach*) potenzialmente significativi [par. 4.2]

Abbiamo condizionato il parere favorevole su uno schema di regolamento (e su un provvedimento ad esso collegato) dell'Ivass in materia di banca dati degli attestati di rischio (assicurativo) ad alcune specificazioni riguardo alle finalità sottese alla trasmissione delle informazioni, alle misure di sicurezza e all'informativa e consenso, nonché la previsione di un termine mas-

simo di conservazione delle informazioni contenute nella banca dati [par. 13.5]

Abbiamo reso parere favorevole su uno schema di decreto del Mef e su un collegato schema di provvedimento del Direttore dell'Agenzia delle entrate i quali, nel rispetto dei suggerimenti formulati dall'Ufficio, definiscono – rispettivamente – le modalità di trasmissione telematica dei dati delle spese sanitarie al Sistema tessera sanitaria ai fini della elaborazione della dichiarazione dei redditi precompilata e le modalità tecniche di utilizzo [parr. 3.4.1 e 4.6]

Abbiamo condizionato il parere sullo schema di decreto del Presidente del Consiglio sui sistemi di sorveglianza e registri di mortalità, di tumori e di altre patologie ad alcune integrazioni del testo, in particolare sulla verifica dell'idoneità dei presupposti legittimanti l'utilizzo a fini di cura dei dati, sull'applicazione delle cautele in materia di protezione dei dati personali e sull'obbligo per i titolari del trattamento di avvisare tempestivamente il Garante nel caso in cui i dati subiscano violazioni (cd. *data breach*) [parr. 3.4.1 e 5.2]

Settembre

Dopo avere esaminato le osservazioni pervenute in sede di consultazione pubblica, abbiamo approvato il codice di deontologia in materia di informazioni commerciali allo scopo di fissare le regole per il corretto uso dei dati sull'affidabilità degli operatori economici, con particolare riguardo alle informazioni contenute nei *report* relativi a imprenditori e *manager* [parr. 13.4 e 19.1]

È stata avviata una consultazione pubblica su uno schema di provvedimento generale relativo al trattamento di dati personali nell'ambito dei servizi di *mobile ticketing*, al fine di definire un quadro coerente di misure a tutela degli utenti e garantire il corretto utilizzo delle informazioni personali trattate [parr. 11.5 e 21.4]

Abbiamo vietato l'ulteriore diffusione sul sito web di un'azienda sanitaria di alcuni provvedimenti relativi alla liquidazione di contributi economici a favore di persone affette da disturbi psichici, contenenti dati idonei a rivelare lo stato di salute e dati eccedenti [par. 4.3]

Ottobre

Tenuto conto delle osservazioni emerse dalla consultazione pubblica del 2014 e dai successivi incontri con le parti coinvolte, abbiamo ritenuto ammissibile la costituzione del "Sistema informativo sulle morosità intenzionali nel settore della telefonia" (S.I.Mo.I.Tel.) ovvero una banca dati delle morosità telefoniche non dovute a difficoltà momentanee, ma ad una precisa volontà dell'utente (con esclusione, invece, delle inadempienze temporanee dovute ad inesperienza, distrazione o difficoltà economiche) [par. 13.3]

Abbiamo dichiarato illecito e vietato ad un'amministrazione carceraria l'ulteriore trattamento per finalità disciplinari dei campioni biologici prelevati alle detenute di una Casa circondariale e dei relativi referti di analisi [par. 8.2]

Abbiamo vietato il trattamento dei dati connesso alle telefonate promozionali effettuate da un *call center* su incarico di una compagnia telefonica in assenza del preventivo consenso dell'utente, il cui numero non risulta presente in elenchi telefonici pubblici (e pertanto impossibilitato ad iscriversi al Registro pubblico delle opposizioni) [par. 11.1]

Abbiamo prescritto ad un'azienda sanitaria di integrare l'informativa e di adottare opportuni accorgimenti per consentire al personale sanitario l'accesso al *dossier* sanitario dei soli pazienti in cura e limitatamente al periodo di terapia. Ciò allo scopo di impedire accessi indiscriminati ai dati dei pazienti e di sanare gravi violazioni riscontra-

te a seguito di accertamenti ispettivi [parr. 5.1.2 e 21.4]

Abbiamo reso parere favorevole su uno schema di regolamento del Miur relativo al trattamento dei dati riferiti alla disabilità degli alunni censiti nell'Anagrafe nazionale degli studenti, condizionandolo all'individuazione di un termine di conservazione congruo e proporzionato dei *log* relativi alla registrazione degli accessi. Per garantire un elevato grado di riservatezza, la documentazione più sensibile – quale la certificazione dello stato di handicap, la diagnosi funzionale, il profilo dinamico funzionale e il piano educativo individualizzato – sarà inserita in una sezione separata e senza il nominativo dell'alunno [parr. 3.4.1 e 4.5]

Novembre

All'esito di verifica preliminare su istanza del Consiglio nazionale del notariato, abbiamo ammesso l'introduzione di un sistema di firma grafometrica idoneo a rafforzare le garanzie di autenticità e integrità dei documenti informatici sottoscritti dagli utenti [par. 14.1]

Abbiamo condizionato il parere favorevole su uno schema di regolamento del Ministero della giustizia recante la disciplina sull'iscrizione telematica degli atti di ultima volontà nel registro generale dei testamenti all'introduzione di una serie di accorgimenti, quali il rafforzamento delle misure di sicurezza e la richiesta di maggiore dettaglio nella regolamentazione della trasmissione e conservazione dei documenti informatici (in considerazione del regime di riservatezza e di segretezza delle informazioni trattate) [par. 3.4.1]

Dicembre

Allo scopo di bloccare eventuali accessi illeciti, abbiamo vietato ad un'azienda sanitaria l'ulteriore diffusione dei dati personali degli utenti registrati sul proprio portale, facilmente conoscibili e modificabili mediante l'utilizzo di una funzione di ricerca presente sul sito [par. 5.1]

Abbiamo ritenuto illecito il trattamento dei dati personali effettuato nel corso di una nota trasmissione radiofonica in ragione delle modalità utilizzate consistenti nel raccogliere telefonicamente dichiarazioni di persone con l'artificio della simulazione di altra identità e nel diffonderle successivamente [par. 9.3]

In materia di scambio automatico obbligatorio di informazioni nel settore fiscale e in linea con i due pareri resi nel mese di luglio sull'Accordo Italia-USA (FATCA) finalizzato a migliorare la *compliance* fiscale internazionale, abbiamo reso parere favorevole su un decreto del Mef concernente le regole tecniche per la rilevazione, la trasmissione e la comunicazione all'Agenzia delle entrate delle informazioni relative ai cittadini di altri Stati esteri, in esecuzione di accordi internazionali [parr. 3.4.1, 4.6 e 22.3]

PAGINA BIANCA

Indice

PAGINA BIANCA

I - LO STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

1. Introduzione: i principali interventi dell'Autorità nel 2015 3

2. Il quadro normativo in materia di protezione dei dati personali 7

2.1. Le novità normative con riflessi in materia di protezione dei dati personali 7

2.1.1. Le leggi di particolare interesse 7

2.1.2. I decreti legislativi 17

3. I rapporti con il Parlamento e le altre Istituzioni 25

3.1. Le segnalazioni al Parlamento e al Governo 25

3.2. Le audizioni del Garante in Parlamento 26

3.3. L'Autorità e le attività di sindacato ispettivo e di indirizzo e controllo del Parlamento 27

3.4. L'attività consultiva del Garante sugli atti del Governo 27

3.4.1. I pareri sugli atti regolamentari e amministrativi del Governo 27

3.4.2. I pareri su norme di rango primario 31

3.5. L'esame delle leggi regionali 32

II – L'ATTIVITÀ SVOLTA DAL GARANTE

4. Il Garante e le pubbliche amministrazioni 37

4.1. I trattamenti di dati sensibili e giudiziari presso le amministrazioni pubbliche 37

4.2. L'amministrazione digitale 37

4.3. La trasparenza amministrativa 40

4.4. La documentazione anagrafica e la materia elettorale 43

4.5. L'istruzione scolastica 46

4.6. L'attività fiscale e tributaria 48

4.7. La videosorveglianza in ambito pubblico 52

4.8. I trattamenti effettuati presso regioni ed enti locali 56

4.9. La previdenza e l'assistenza sociale 58

4.10. L'attività giudiziaria 62

5. La sanità 65

5.1. I trattamenti per fini di cura 65

5.1.1. L'informativa e il consenso al trattamento dei dati sanitari 66

Indice

5.1.2. Il Fascicolo sanitario elettronico e i dossier *sanitari* 66
5.1.3. I referti e la documentazione sanitaria 68
5.1.4. La tutela della dignità della persona 69
5.1.5. Il trattamento di dati personali concernente l'accertamento dell'infezione da HIV 70
5.2. I trattamenti di dati sanitari per fini amministrativi 71
5.2.1. L'attività consultiva sugli atti regolamentari e amministrativi del Ministero della salute 74

6. I dati genetici 80

7. La ricerca scientifica e la statistica 83
7.1. La ricerca scientifica 83
7.2. La statistica 84

8. I trattamenti da parte di Forze di polizia 89
8.1. Il controllo sul Ced del Dipartimento della pubblica sicurezza 89
8.2. Altri interventi riguardanti le Forze di polizia 89
8.3. Il controllo sul sistema di informazione Schengen 93

9. L'attività giornalistica 94
9.1. Le persone decedute 94
9.2. La cronaca giudiziaria 95
9.3. I personaggi pubblici 95
9.4. Gli archivi storici e le informazioni *online* 96

10. Il trattamento di dati personali attraverso internet 98
10.1. L'informativa e consenso per il trattamento dei dati personali mediante i siti web 98
10.2. Le Linee guida in materia di trattamento di dati personali per profilazione *online* 98
10.3. La consultazione pubblica su *Internet of Things* 99

11. Il trattamento di dati personali nel settore delle comunicazioni elettroniche 101
11.1. Le telefonate promozionali indesiderate 101
11.2. I trattamenti di dati personali effettuati mediante *call center* ubicati al di fuori dell'Unione europea 102
11.3. I dati personali utilizzati a fini di *marketing* e profilazione 102
11.4. Le verifiche preliminari *ex* art. 17 del Codice 103
11.5. Il *mobile ticketing* 106

11.6. Il contrasto allo *spam* 106
11.6.1. Trattamento per finalità promozionali di dati personali estratti dal database della mobile number portability 107
11.7. Le notificazioni di *data breach* 107
11.8. *Data retention* 108
11.9. La geolocalizzazione di *smartphone* di persone disperse 108

12. La protezione dei dati personali nel rapporto di lavoro pubblico e privato 110
12.1. I controlli a distanza mediante videosorveglianza 110
12.2. I controlli sull'utilizzo di posta elettronica aziendale e di internet 112
12.3. Il trattamento di dati personali nella gestione del rapporto di lavoro 113
12.4. La pubblicità e trasparenza dei dati dei lavoratori 114
12.5. La pubblicazione *online* di dati idonei a rivelare la condizione di disabilità 115
12.6. I quesiti in materia di trasparenza 115
12.7. La comunicazione tra soggetti pubblici di dati relativi ai lavoratori 117

13. Le attività economiche 118
13.1. Il settore bancario 118
13.2. La revisione del codice deontologico Sic 118
13.3. Il fenomeno delle morosità nel settore delle cd. *utilities* 119
13.4. Il nuovo codice di deontologia e di buona condotta in materia di informazioni commerciali 121
13.5. Il settore assicurativo 122
13.6. La videosorveglianza in ambito privato 123
13.7. Il recupero crediti 123
13.8. Altre attività imprenditoriali 124

14. I dati biometrici 126
14.1. Il trattamento dei dati biometrici nel settore societario e professionale 126
14.2. Il trattamento dei dati biometrici nel rapporto di lavoro 127

15. Attività di normazione tecnica internazionale e nazionale 129

16. Il trattamento dei dati nel condominio 130

17. Il trasferimento dei dati all'estero 131

Indice

18. Il registro dei trattamenti 133

18.1. La notificazione 133

18.2. L'evoluzione della notificazione nel 2015 133

19. La trattazione dei ricorsi 136

19.1. I profili generali 136

19.2. I dati statistici 137

19.3. La casistica più significativa 137

20. Il contenzioso giurisdizionale 140

20.1. Considerazioni generali 140

20.2. I profili procedurali 140

20.3. Le opposizioni ai provvedimenti del Garante 141

20.4. L'intervento del Garante nei giudizi relativi all'applicazione del Codice 147

21. L'attività ispettiva e le sanzioni 148

21.1. La programmazione dell'attività ispettiva 148

21.2. La collaborazione con la Guardia di finanza 149

21.3. I principali settori oggetto di controllo 150

21.4. I provvedimenti adottati dall'Autorità a seguito dell'attività ispettiva 152

21.5. L'attività sanzionatoria del Garante 154

21.5.1. Le violazioni penali e i procedimenti relativi alle misure minime di sicurezza 154

21.5.2. Le sanzioni amministrative 156

22. Le relazioni comunitarie e internazionali 161

22.1. La riforma del quadro giuridico europeo in materia di protezione dei dati 162

22.2. Le conferenze delle Autorità su scala internazionale 168

22.3. La cooperazione tra Autorità garanti nell'UE: il Gruppo Art. 29 169

22.4. La cooperazione delle Autorità di protezione dei dati nel settore libertà, giustizia e affari interni 177

22.5. La partecipazione ad altri comitati e gruppi di lavoro internazionali 181

23. L'attività di comunicazione, informazione e di rapporto con il pubblico 186

23.1. La comunicazione del Garante: profili generali 186

23.2. I prodotti informativi 187
23.3. I prodotti editoriali e multimediali 188
23.4. Le manifestazioni e le conferenze 189
23.5. Le relazioni con il pubblico 191

24. Studi, documentazione e trasparenza 195
24.1. Il Servizio studi e documentazione 195
24.2. La biblioteca 196
24.3. L'Autorità trasparente 197

III – L'UFFICIO DEL GARANTE

25. La gestione amministrativa e dei sistemi informatici 203
25.1. Il bilancio e la gestione finanziaria 203
25.2. L'attività contrattuale e la gestione economale 204
25.3. Le novità legislative, regolamentari e l'organizzazione dell'Ufficio 206
25.4. Il personale e i collaboratori esterni 208
25.5. Il settore informatico e tecnologico 209

IV – I DATI STATISTICI 213

Avvertenza ed elenco delle abbreviazioni

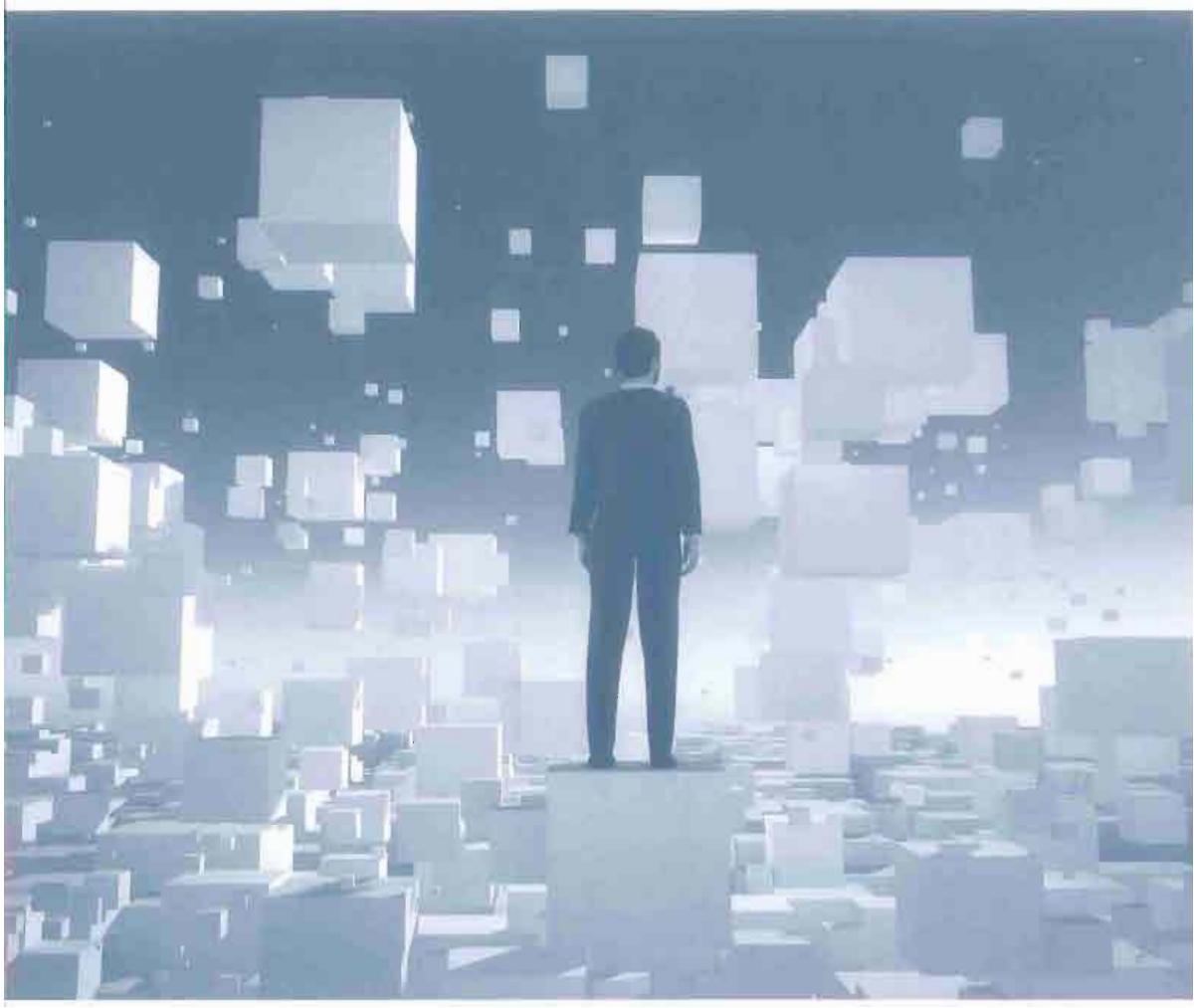
La presente Relazione è riferita al 2015 e contiene talune notizie già anticipate nella precedente edizione nonché informazioni relative a sviluppi che si è ritenuto opportuno menzionare.

AgID	Agenzia per l'Italia Digitale
All.	Allegato
Anac	Aurorità nazionale anticorruzione
Anpr	Anagrafe nazionale della popolazione residente
art.	articolo
Asl	Azienda saniraria locale
c.c.	codice civile
C.d.S.	Consiglio di Stato
c.p.	codice penale
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
cap.	capitolo
cd.	cosiddetto/i
cfr.	confronta
CGUE	Corte di giustizia dell'Unione europea
cit.	citato
Codice	Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196)
Corte EDU	Corte europea dei diritri dell'uomo
Cost.	Costituzione
d.d.l.	disegno di legge
d.l.	decrero-legge
d.lgs.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei Minisrri
d.P.G.p.	decreto Presidente Giunta provinciale
d.P.R.	decreto del Presidenre della Repubblica
doc.	documento
es.	esempio
GU	Gazzetta Ufficiale della Repubblica italiana
GUUE	Gazzetta Ufficiale dell'Unione europea
Gruppo Art. 29	Gruppo dei garanti europei istituto dall'art. 29 della direttiva 95/46/CE
l.	legge

lett.	lettera
n.	numero
p.	pagina
p.a.	pubblica amministrazione
par.	paragrafo
Pec	posta elettronica certificata
provv.	provvedimento del Garante
r.d.	regio decreto
reg.	regolamento
sez.	sezione
Ssn	Servizio sanitario nazionale
tab.	tabella
t.u.	testo unico
TFUE	Trattato sul funzionamento dell'Unione europea
UE	Unione europea
url	*Uniform Resource Locator*
v.	vedi

PAGINA BIANCA

Stato di attuazione del Codice in materia di protezione dei dati personali



PAGINA BIANCA

I – Stato di attuazione del Codice in materia di protezione dei dati personali

1 Introduzione: i principali interventi dell'Autorità nel 2015

1.1. Una rapida panoramica sull'attività svolta dall'Autorità nel corso del 2015 (di seguito meglio illustrata) riserva certamente uno spazio di rilievo ai lavori tesi a supportare, dopo ben quattro anni, la conclusione dell'*iter* legislativo del regolamento generale sulla protezione dati e della direttiva sulla protezione dati nelle atrività giudiziarie e di polizia (cd. pacchetto protezione dati) adottati dal Parlamento europeo e dal Consiglio, la cui pubblicazione è prevista sulla GUUE del 4 maggio 2016. Si tratta di un traguardo molto atteso, punto di arrivo di una complessa procedura legislativa che l'Autorità ha seguito sin dall'inizio partecipando attivamente – nelle diverse sedi istiruzionali – al vivace ed articolato dibattito che ha portato alla definizione dei testi. Regolamento e direttiva, nella versione definitiva adottata, andranno a innovare (anche per effetto della prevista abrogazione della direttiva 95/46/CE e della decisione quadro 2008/977/GAI del Consiglio) il quadro normativo comunitario e nazionale in modo uniforme ed armonico a tutti gli Stati membri (par. 22.1).

In ambito comunitario metita altresì un cenno, in ragione della potenzialità degli effetti sul trasferimento dei dati tra UE e USA, la sentenza della Corte di giustizia del 6 ottobre 2015 (causa C-362/14, Maximillian Schrems/Data Protection Commissioner) con la quale è stata dichiarata invalida la decisione della Commissione del 26 luglio 2000 relativa alla valutazione di adeguatezza del livello di protezione dati garantito dagli Stati Uniri nel contesto del cd. regime di "approdo sicuro" (*Safe Harbor*). A seguito della pronuncia, oltre alle prime indicazioni sul trasferimenro dei dati verso gli Stati Uniti rese dai Garanti europei riuniti nel Gruppo Art. 29, l'Autorità ha provveduto a disporre la caducazione dell'autorizzazione del 2001 che "aveva recepito" la decisione della Commissione dichiarata invalida (cap. 17).

1.2. Un peso altrettanto ragguardevole ha rivestito l'impegno con il quale l'Autorità ha collaborato con il Governo e le altre Amministrazioni attraverso la formulazione di pareri sugli atti normativi. L'attività consultiva dell'Aurorità, tradizionalmente rilevante dal punto di vista quantitativo, ha registrato nel 2015 un sostanziale raddoppio (cfr. sez. IV, tab. 3) anche per effetto dei processi di riforma in atto su importanti ambiti pubblici e privati.

I pareri resi hanno riguardato tematiche molto diverse, spesso attinenti a complessi profili tecnologici e a settori emergenti (par. 3.4.1), quali i sistemi informativi in ambito sanitario – si pensi all'interconnessione a livello nazionale dei sistemi

informativi su base individuale del Ssn, ai flussi informativi dei pazienti dimessi dagli istituti di ricovero pubblici e privati, al Sistema informativo trapianti e ai registri di mortalità – (par. 5.2.1), quelli in ambito previdenziale ed assistenziale (par. 4.9) e in ambito scolastico ivi compreso il trattamento dei dati sulle disabilità degli alunni censiti nell'Anagrafe nazionale degli studenti (Ans) e l'integrazione dell'Ans con i dati relativi agli iscritti alla scuola dell'infanzia (par. 4.5); l'attuazione della normativa FATCA relativa allo scambio automatico ed obbligatorio di informazioni fiscali tra Italia e USA finalizzata al miglioramento della *compliance* fiscale (parr. 4.6. e 22.3); il censimento della popolazione e il Programma statistico nazionale (Psn) (par. 7.2); l'accesso alla dichiarazione 730 precompilata e la trasmissione telematica delle spese sanitarie al Sistema tessera sanitaria (par. 4.6) nonché, con riguardo alla riorganizzazione delle amministrazioni pubbliche, il permesso di soggiorno elettronico (Pse) e, con quattro distinti pareri, l'attuazione del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (Spid) (parr. 2.1 e 4.2). L'Autorità è inoltre ripeturamente intervenuta in sede consultiva sul processo di modernizzazione della giustizia, con specifico riguardo all'attuazione del processo telematico (ordinario, amministrativo, contabile e tributario) e all'implementazione dei sistemi informativi (albo degli amministratori giudiziari e posta elettronica certificata).

1.3. Il Garante ha indirizzato al Parlamento e al Governo segnalazioni (cfr. par. 3.1) relative alla necessità di integrare o modificare i testi normativi rilevanti sotto il profilo della protezione dati, come nel caso delle segnalazioni sulla razionalizzazione del sistema sanzionatorio previsto dal Codice e sull'installazione della cd. scatola nera sui veicoli (entrambe già oggetto di similare intervento nel 2014), nonché sulle possibili implicazioni – in ordine al rispetto dei parametri costituzionali e ad un'eventuale disparità di trattamento tra i cittadini – derivanti dalle leggi regionali in materia di trasparenza amministrativa "in deroga" alla normativa statale (d.lgs. n. 33/2013).

Finalità di collaborazione istituzionale hanno altresì rivestito le audizioni rese dall'Autorità in Parlamento (par. 3.2) e gli atti di sindacato ispettivo, di indirizzo e conttollo su profili e settori di interesse (par. 3.3). Inoltre, in continuità con l'attività svolta dall'Autorità lo scorso anno (v. Relazione 2014, p. 194) - e con i lavori della Commissione di studio parlamentare conclusisi, nel corso del 2015, con l'approvazione e la pubblicazione della Dichiarazione dei Diritti in Internet - è stata avviata una consultazione pubblica sulle nuove tecnologie classificabili come *Internet of Things* ovvero sui rischi per la protezione dei dati connessi all'interconnessione di oggetti e sistemi diversi quali pc, *smartphone* e oggetti di uso quotidiano (par. 10.3).

1.4. La rete e le sue molteplici sfaccettature hanno continuato ad essere oggetto dell'attenzione dell'Autorità la quale, nel mese di gennaio, ha dedicato a questa tematica il convegno celebrativo della IX Giornata europea della protezione dei dati personali. "Il pianeta connesso. La nuova dimensione della *privacy*" è stato il tema prescelto per la consueta occasione di riflessione ed analisi sulle problematiche afferenti alla protezione dati, approfondendo in particolare la difesa dei diritti delle persone nella cd. infosfera quale *habitat* popolato di dati, informazioni ed esperienze condivise (par. 23.4). Apposite Linee guida sono state adottate per individuare le regole che i fornitori di servizi *online* devono rispettare per le attività di profilazione allo scopo di garantite maggiori tutele agli utenti (in particolare obbligatorietà dell'informativa e del consenso con riguardo a tutte le modalità di trattamento, par. 10.2), e ha vietato il trattamento dei dati per finalità promozionali e di profilazione non conforme

alla normativa, prescrivendo l'adozione delle misure necessarie (par. 11.3).

Sempre con riguardo alla rete il Garante, a seguito della sentenza della CGUE nel caso Google Spain, è ripetutamente intervenuto sulle richieste di deindicizzazione di pagine web riportanti informazioni personali valutate prive di interesse pubblico (par. 19.3) e con provvedimenti di contrasto allo *spam* (par. 11.6). In tale contesto merita un cenno l'indagine connessa allo *Sweep day* 2015 promossa dal *Global Privacy Enforcement Network* (GPEN) e dedicata alla protezione in rete dei bambini tra gli 8 e i 13 anni. L'esito dell'analisi condotta sui siti internet più visitati e sulle *app* (scaricabili su *smartphone* e *tablet*) più diffuse, analogamente a quanto riscontrato dalla altre Autorità aderenti all'iniziativa, ha fatto emergere un quadro di scarsa tutela nei confronti dei più piccoli con punte di gravi criticità sulle quali il Garante si è riservato azioni ed approfondimenti anche di tipo ispettivo (par. 22.5).

1.5. È stato seguito con particolare impegno il settore della sanità e, in tale ambito, il vigente processo di ammodernamento volto a migliorare la qualità del servizio sanitario e a semplificare l'esercizio del diritto alla salute anche attraverso il ricorso alle più avanzate tecnologie informatiche. Oltre ai pareri a cui si è fatto cenno *supra* e meglio esaminati nel par. 5.2.1, in continuità con l'attività svolta nel corso dell'anno precedente sul Fascicolo sanitario elettronico (cfr. Relazione 2014, p. 60), meritano una menzione le Linee guida in materia di *dossier* sanitario elettronico (prezioso strumento per la diagnosi e cura dei pazienti) finalizzate a garantire una maggiore tutela agli utenti (ad es., attraverso il riconoscimento in capo al paziente del diritto ad accedere agli accessi effettuati al proprio *dossier*) e a rendere più sicuto, anche sotto il profilo della protezione dati, l'utilizzo dei *dossier* sanitari (par. 5.1.2). Inoltre numerosi sono stati gli interventi prescrittivi ed inibitori sui trattamenti dei dati sanitari tra i quali si citano, a titolo meramente esemplificativo, quelli relativi agli accessi indiscriminati ai dati dei pazienti, alla consegna dei referti e della documentazione sanitaria o all'accertamento dell'infezione da HIV (par. 5.1.5). Gli interventi dell'Autorità hanno riguardato anche l'uso di dati sanitari in contesti diversi da quelli strettamente ospedalieri, come nel caso dei divieti formulati rispettivamente ad un'amministrazione carceraria di utilizzare i campioni biologici prelevati alle detenute per finalità disciplinari (par. 8.2) e ad una Regione di diffondere i dati dei partecipanti ad una iniziativa pubblica riservata a disabili (par. 4.3).

Per quanto attiene invece ai dati genetici (cap. 6.), il Garante è intervenuto, a seguito degli accertamenti svolti lo scorso anno (cft. Relazione 2014, p. 71), sulla cessione a terzi di una banca dati genetica (richiamando in particolare l'osservanza del principio di finalità ai fini dell'efficacia dell'atto di trasferimento e dell'utilizzabilità dei dati trasferiti) e sull'istituzione delle biobanche di ricerca previste da una legge regionale sulla quale la Presidenza del Consiglio dei ministri aveva chiesto elementi di valutazione ai fini dell'eventuale impugnazione davanti alla Corte costituzionale (rilevando criticità sull'omessa previsione delle specifiche finalità del trattamento e delle fonti del materiale biologico, poi superate da una successiva legge della medesima Regione).

1.6. Con riguardo alla protezione dei dati personali dei lavoratori e nel tentativo di fornire un contributo utile all'individuazione di un ragionevole equilibrio tra le ragioni datoriali e la tutela del lavoratore, l'Autorità ha manifestato, in sede di lavori parlamentari, le proprie preoccupazioni in merito alla novella sulla disciplina del controllo a distanza dei lavorarori introdotta da un decreto di attuazione del cd. *Jobs Act* ed in particolare sull'estensione dell'utilizzabilità dei dati raccolti (cap. 12). Allo scopo di impedire ingiustificate forme di controllo, l'Autorità è

intetvenuta con prescrizioni e divieti in numerosi casi relativi, tra l'altro, all'indebito utilizzo di posta elettronica aziendale e di internet (come nel caso dei trattamenti effettuati da una società in relazione alle conversazioni Skype dei dipendenti e soggetti terzi; cfr. par. 19.3), a trattamenti di dati biometrici dei lavoratori per finalità di sicurezza (come nel caso del sistema biometrico utilizzato da un Comune per la rilevazione delle presenze dei dipendenti; cfr. par. 14.2) nonché a trattamenti di dati dei lavoratori mediante videosorveglianza (come nel caso dei sistemi di videosorveglianza all'interno delle auto e di localizzazione dei palmari in dotazione ai dipendenti utilizzati da un consorzio di polizia locale; cfr. par. 12.1).

1.7. Numerosi sono stati nel corso dell'anno gli interventi nel settore bancario anche per effetto della persistente crisi economico-finanziaria e dei recenti casi di "criticità" di banche e istituti di credito. Centrale è stata l'attenzione al tema delle grandi banche dati nel cui ambito possono annoverarsi la prosecuzione dei lavori di revisione del codice di deontologia dei sistemi di infotmazione creditizia (Sic), la costituzione di una banca dati relativa a morosità intenzionali della clientela del settore telefonico (S.I.Mo.I.Tel.) e l'adozione del codice di deontologia e di bnona condotta per il trattamento dei dati personali effettuato ai fini di informazione commerciale (cap. 13).

La tutela dei dati personali dei consumatori è stata oggetto di attenzione nelle prescrizioni impartite ad una società televisiva per il recupero degli importi insoluti dei clienti (par. 13.7), nel documento sui servizi di *mobile ticketing* sottoposto a consultazione pubblica (par. 11.5) nonché negli atti – anche di natura sanzionatoria – adottati a seguito delle comunicazioni di avvenuti *data breach* da parte dei più importanti fornitori nazionali di servizi di comunicazione elettronica (par. 11.7.)

1.8. L'Autorità ha continuato a perseguire gli obiettivi di risparmio e contenimento della spesa indicati, tra l'altro, dalla normativa sulla *spending review* anche a mezzo della riduzione del trattamento economico accessorio del personale dipendente e l'avvio della gestione di alcuni servizi in comune con altre antorità amministrative indipendenti (part. 25.1 e 25.2). Ciò stante la perdurante preoccupazione relativa alla grave inadeguatezza, a legislazione vigente, dell'attuale sistema di finanziamento dell'Autorità (oggetto di progressivo depauperamento nel corso degli ultimi anni) e prossimo a cessare di produrre effetti in misura molto consistente, tanto da rischiare di pregiudicare (se non adeguatamente reintegrato) la regolare prosecuzione dell'attività istituzionale (cfr. sez. IV, tab. 19). Pur in tale angusto contesto, il Garante ha continuato ad assolvere i propri compiri anche attraverso il consolidamento dell'attività di comunicazione istituzionale ritenuta da sempre fondamentale per la diffusione di una cultnra della protezione dei dati (par. 23.1 e sez. IV, tab. 2), una proficua attività ispettiva in *loco* (cap. 21), effettuata anche grazie alla preziosa e collaudata collaborazione della Guardia di finanza ed in particolare del Nucleo speciale *privacy* (cfr. sez. IV, tab. 6) nonché un'attenta attività sanzionatoria i cui cospicui proventi sono stati versati sul bilancio dello Stato (cfr. sez. IV, tab. 8).

1.9. Da quanto sinteticamente rappresentaro, si auspica potersi ricavare l'impegno e l'energia con i quali l'Autorità ha continuato a raccogliere, nel corso dell'anno, le ambiziose sfide dettate da un incalzante progresso tecnologico e da una società digirale *in divenire*, nonché l'ulteriore investimento che sarà necessario – nei prossimi mesi ed anni – per assolvere ai nuovi ed importanti compiti che il cd. pacchetto protezione dati affida al Garante, anche in condivisione con le altre autorità nazionali di protezione dati.

2 Il quadro normativo in materia di protezione dei dati personali

2.1. *Le novità normative con riflessi in materia di protezione dei dati personali*

2.1.1. Le leggi di particolare interesse

Nel 2015 sono stati approvati numerosi provvedimenti normativi che hanno riflessi in materia di protezione dei dati personali. Fra questi, al fine di offrirne una sintetica ricognizione, tale da rendere conto dell'ampiezza e dell'eterogeneità delle materie che rientrano nell'area di interesse dell'Autorità, si menzionano in particolare:

Riforma della RAI

1) la legge 28 dicembre 2015, n. 220 recante riforma della RAI e del servizio pubblico radiotelevisivo che reca una disposizione in materia di trasparenza (art. 2, comma 10, lett. *g*), n. 2), a norma della quale il piano per la trasparenza e la comunicazione aziendale deve prevedere le forme più idonee per rendere conoscibili alla generalità degli utenti le informazioni sull'attività complessivamente svolta dal consiglio di amministrazione, salvi casi particolari di riservatezza adeguatamente motivati. La menzionata norma prevede in particolare la pubblicazione nel sito internet della società, fra l'altro, dei *curricula* e dei compensi lordi, comunque denominati, percepiti dai componenti degli organi di amministrazione e controllo, dai dirigenti di ogni livello, e comunque dai soggetti, diversi dai titolari di contratti di natura artistica, che ricevano un trattamento economico annuo omnicomprensivo a carico della società pari o superiore ad euro 200.000, con indicazione delle eventuali componenti variabili o legate alla valutazione del risultato, nonché delle informazioni relative allo svolgimento da parte dei medesimi di altri incarichi o attività professionali ovvero alla titolarità di cariche in enti di diritto privato regolati o finanziati dalle pp.aa., ivi comprese le autorità amministrative indipendenti;

Missioni internazionali

2) il decreto-legge 30 ottobre 2015, n. 174, recante Proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione, convertito dalla l. 11 dicembre 2015, n. 198, il quale prevede che l'ammontare del trattamento economico e delle spese per vitto, alloggio e viaggi del personale del Ministero degli affari esteri, inviato per la partecipazione alle operazioni internazionali in aree di crisi, siano resi pubblici per garantire la trasparenza, nel rispetto della vigente legislazione in materia di protezione dei dati personali (art. 9, comma 6);

Riorganizzazione delle amministrazioni pubbliche

3) la legge 7 agosto 2015, n. 124 con la quale il Parlamento ha assegnato al Governo un compito vasto e delicato nella riorganizzazione dello Stato e degli altri organismi pubblici (Capo II), nonché in materia di personale (Capo III), di lavoro dipendente e di servizi pubblici (Capo IV), attraverso importanti deleghe da esercitare in chiave di razionalizzazione del sistema e di semplificazione amministrativa, anche per quanto riguarda l'anticorruzione, la pubblicità e la trasparenza (Capo I). Alcune di queste deleghe – come vedremo meglio più avanti – sono di estremo interesse per l'Autorità in particolare quelle per: la revisione e semplificazione delle disposizioni in materia di pubblicità di atti e documenti e di trasparenza (art. 7); la razionalizzazione del sistema al fine di evitare sovrapposizione di compiti e funzioni fra uffici ministeriali e autorità indipendenti e per l'individuazione di criteri omogenei per il finanziamento di queste ultime (art. 8, comma 1, lett. *c*), n. 6); l'istitu-

zione del "sistema della dirigenza pubblica", con espresso riferimento alla "dirigenza delle autorità indipendenti" e all'introduzione di "ruoli unici" (art. 11); l'attuazione della Carta della cittadinanza digitale (art. 1). A tal proposito, data la delicatezza delle materie interessate e l'incidenza delle deleghe sulla materia della protezione dei dati personali e sulle autorità indipendenti, il Garante ha tempestivamente rappresentato al Ministro per la semplificazione e la funzione pubblica la più ampia disponibilità a collaborare nella fase di attuazione della legge.

Più nel dettaglio si illustrano i principali profili di interesse per l'Autorità:

Le autorità indipendenti e il loro finanziamento

a) occorre premettere che l'originario impianto del d.d.l. all'art. 8 recava le definizioni dei soggetti coinvolti dalla riforma, funzionali all'individuazione dell'ambito di applicazione delle disposizioni normative in esame, posta la ricorrente non univocità di richiami normativi nel corpo della legislazione. Le diverse categorie di amministrazioni erano così denominate dall'articolo: amministtazioni statali; amministrazioni nazionali; amministtazioni tertitoriali; amministrazioni di istruzione e cultura; amministrazioni pubbliche; soggetti di rilievo pubblico; organismi privati di interesse pubblico. Premesso che fra le amministrazioni statali si comprendevano la Presidenza del Consiglio dei ministri, l'amministrazione del Consiglio di Stato, della Corte dei conti e dell'Avvocatura dello Stato, i Ministeri, le agenzie fiscali, le altre agenzie incluse quelle istituite *ex* d.lgs. n. 300/1999, escluse le amministrazioni di istruzione e cultura, le amministrazioni nazionali ivi comprese le autorità indipendenti. Le amministrazioni nazionali, unitamente a quelle territoriali, di istruzione e cultura, nonché agli ordini professionali, facevano parte della più ampia categoria delle amministrazioni pubbliche. Al contempo, si prevedeva che con d.P.R. si redigesse un elenco, aggiornato annualmente, per ciascuna categoria (art. 8, comma 3). Il menzionato articolo, è stato soppresso nel corso dell'esame in prima lettura in Commissione affari costituzionali del Senato nonostante, come rilevato nella relazione illustrativa del d.d.l., la finalità della norma fosse quella di dare una base legislativa alla definizioni che individuano le amministrazioni pubbliche, senza dover ricorrere a specifici rinvii ad altre disposizioni. La mancanza nell'articolato di tale disposizione definitoria toglie certezza all'ambito applicativo della legge, lasciando al contempo inalterati (o comunque non estinguendo del tutto) i dubbi interpretativi in punto di riferibilità delle norme alle autorità indipendenti. Come si vedrà più avanti, infatti, la delega per il riordino della disciplina del lavoro dipendente riguarda le amministrazioni pubbliche di cui non c'è più, però, una definizione. Resta confermato, in ogni caso, che le autorità indipendenti non fanno parte dell'amministrazione dello Stato, come si evince dalla delega per il riordino di quella amministrazione. L'art. 8 della legge (già art. 7 del d.d.l.), infatti, delega il Governo ad adottare decreti legislativi per modificare la disciplina della Presidenza del Consiglio dei ministri, dei Ministeri, delle agenzie e degli enti pubblici non economici nazionali. In particolare, la lett. *c*) indica princìpi e criteri riferiti esclusivamente alla riorganizzazione dell'amministrazione centrale, concentrati in particolar modo al rafforzamento del ruolo di indirizzo e coordinamento del Presidente del Consiglio dei ministri e sulle correlate funzioni della Presidenza del Consiglio dei ministri. Quel che più conta ai nostri fini è che tra i princìpi e i criteri direttivi cui il Governo dovrà uniformarsi vi è anche – sin dalla stesura originaria del d.d.l. – la "razionalizzazione con eventuale soppressione degli uffici ministeriali le cui fun-

zioni si sovrappongono a quelle delle autorità indipendenti" (art. 8, comma 1, lett. *c*), n. 6). A tal proposito, si evidenzia un'integrazione apportata dalla Camera al predetto criterio di delega (emendamento 7.501 della Commissione affari costituzionali approvato dall'Assemblea), in base alla quale la menzionata "razionalizzazione con eventuale soppressione degli uffici ministeriali le cui funzioni si sovrappongono a quelle delle autorità indipendenti" dovrà avvenire anche "e viceversa". Inoltre, a seguito dell'emendamento, si richiede l'individuazione di criteri omogenei per la determinazione del trattamento economico dei componenti e del personale delle autorità indipendenti, "salvaguardandone la relativa professionalità", nonché per il finanziamento di queste ultime, in modo da non gravare sulla finanza pubblica. La nuova disposizione introdotta precisa poi che l'individuazione dei criteri per il finanziamento deve avvenire "mediante la partecipazione, ove non attualmente prevista, delle imprese operanti nei settori e servizi di riferimento, o comunque regolate o vigilate". Infine, si sottolinea l'accoglimento da parte del Governo, nella seduta conclusiva del 17 luglio scorso, di un ordine del giorno (9/3098-A/82, a firma dell'on. Bruno Bossio), con cui s'impegna ad adottare ogni più adeguato intervento applicativo volto ad assicurare la coerenza nella fase di attuazione della disposizione in esame, salvaguardando le "rispettive specificità e professionalità" delle autorità; ciò, tenuto conto della *ratio* della norma di realizzare un tendenziale allineamento dei trattamenti economici del personale di tali soggetti, voluti come distinti dal "comparto ministeri" sin dalla loro istituzione, in ragione delle loro peculiarità ed autonomia, anche finanziaria.

Disposizioni sul personale

b) Il Capo III detta disposizioni sul personale e, in particolare, sulla dirigenza pubblica (art. 11, l. n. 124/2015), prevedendo l'istituzione del "sistema della dirigenza pubblica", articolato in ruoli unificati e coordinati, accomunati da requisiti omogenei di accesso e da procedure analoghe di reclutamento, basati sul principio del merito, dell'aggiornamento e della formazione continua nonché su quello della "piena mobilità tra i ruoli" (art. 11, comma 1, lettera *a*). Viene dunque istituito un ruolo unico dei dirigenti statali presso la Presidenza del Consiglio, in cui confluiscono i dirigenti di cui all'art. 2, comma 2, d.lgs. n. 165/2001 appartenenti alle amministrazioni statali (art. 11 lett. *b*), n. 1). La norma di delega fa riferimento espressamente, in alcuni casi, alla "dirigenza delle autorità indipendenti", come, ad es., a proposito dell'introduzione di "ruoli unici". Al riguardo, peraltro, si apprezza la modifica introdotta in Commissione al Senato in base alla quale, i predetti ruoli unici potranno essere introdotti solo "nel rispetto della loro piena autonomia". Sarà compito della normativa delegata declinare in concreto l'ambito di tale riconosciuta autonomia alle autorità indipendenti. Altro riferimento espresso alle autorità indipendenti è quello riguardante il reclutamento della dirigenza, che potrà avvenire con il corso-concorso o il concorso anche per i dirigenti delle autorità indipendenti (art. 11, comma 1, lett. *c*), nn. 1 e 2). Da questo punto di vista si apprezza la chiarezza descrittiva dell'articolo in esame, che conferma la distinzione fra "dirigenza statale" e "dirigenza delle autorità indipendenti". La medesima diversificazione terminologica manca invece rispetto agli altri criteri di delega dell'art. 11, che sono riferiti genericamente alla "dirigenza pubblica". Si tratta delle disposizioni concernenti la formazione, il conferimento e la durata degli inca-

richi, la disciplina dei dirigenti privi di incarico, la valutazione dei risultati e la responsabilità dei dirigenti (art. 11, comma 1, lettere da *d*) a *q*). A tal riguardo, con un emendamento apptovato alla Camera (9.1001) è stato specificato che dal "ruolo unico dei dirigenti statali" è escluso il personale cd. non contrattualizzato in regime di diritto pubblico, di cui all'art. 3, d.lgs. n. 165/2001 (nel testo originario era invece contemplata la confluenza in tale ruolo del personale appartenente alle carriere speciali, ad esclusione di quella diplomatica). Si rammenta, in proposito, che il predetto art. 3, al comma 1, fa riferimento ai magistrati ordinari, amministrativi e contabili, agli avvocati e procuratori dello Stato, al personale militare e delle Forze di polizia di Stato, della carriera diplomatica e prefettizia, del Corpo nazionale dei vigili del fuoco, della carriera dirigenziale penitenziaria, ai professori e ricercatori universitari, ma anche al personale di alcune autorità indipendenti. È evidente però che il richiamo a fini di esclusione dal ruolo unico in questione va limitato al solo personale della dirigenza statale (mentre il ruolo unico della dirigenza delle autorità indipendenti è disciplinato a parte, come detto sopra, e riguarda tutte le *authority*). Ciò premesso, nel merito delle disposizioni dell'art. 11, la riferibilità dell'intero articolo ai dirigenti delle autorità indipendenti dovrebbe comportare la loro partecipazione alla prevista "piena mobilità" fra tutti i ruoli della dirigenza pubblica. Rilevante inoltre è la disposizione che prevede l'"omogeneizzazione" del trattamento economico fondamentale e accessorio nell'ambito di ciascun ruolo unico (lett. *n*). Quanto all'impatto sulla normativa in materia di protezione dei dati personali, si evidenziano:

- l'istituzione di una banca dati, la cui gestione è affidata al Dipartimento della funzione pubblica, in cui inserire *curriculum vitae* e profilo professionale per ciascun dirigente, inclusi gli esiti delle valutazioni ottenute (art. 11, comma 1, lett. *a*);
- la possibilità per il dirigente di attribuire un premio monetario annuale al personale, pubblicando nel sito istituzionale l'identità dei destinatari dei premi (lett. *n*).

Deleghe in materia di lavoro, partecipazioni societarie e servizi pubblici

c) Nel Capo III inoltre si delega il Governo ad adottare decreti legislativi di semplificazione in tre settori: lavoro alle dipendenze delle "amministrazioni pubbliche" e connessi profili di "organizzazione amministrativa", partecipazioni societarie delle amministrazioni pubbliche e servizi pubblici locali (art. 16). In quest'ultimo caso, tra i princìpi e criteri direttivi per il decreto legislativo di riordino della materia si prevede la "individuazione e allocazione dei poteri di regolazione e controllo fra i diversi livelli di governo e le autorità indipendenti", fra le quali non dovrebbe essere ricompreso il Garante, *ratione materiae* (art. 19, comma 1, lett. *n*). Di un certo interesse per l'Autorità è il primo settore (art. 17), sebbene resti dubbia la sua riferibilità al personale delle autorità indipendenti, stante il fatto che il disegno di legge non reca più – come abbiamo precisato sopra – le definizioni dei soggetti facenti parte del settore pubblico.

Prevenzione della corruzione, pubblicità e trasparenza

d) La legge contiene numerose disposizioni finalizzate a semplificare i servizi per cittadini e imprese, in materia di conferenza di servizi, silenzio assenso, segnalazione certificata di inizio attività, autotutela amministrativa e anticorruzione, pubblicità e trasparenza. Particolarmente importante è l'art. 7 recante una delega per la revisione e la semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza,

mediante modifiche e integrazioni al d.lgs. n. 33/2013. L'articolo è stato modificato al Senato, e poi praticamente riscritto in Commissione affari costituzionali della Camera, a seguito dell'approvazione di alcuni emendamenti parlamentari (in particolare, 6.69 e 6.70) e del relatore (6.71). Dalla ricostruzione del nuovo articolo emerge con evidenza che la delega non riguarda più il d.lgs. n. 39/2013 in materia di incarichi presso le pp.aa., ma solo il d.lgs. n. 33.

Fra i criteri di delega – significativamente modificati e integrati (lettere da *a*) a *h*) del comma 1) si segnalano:

a) "ridefinizione e precisazione dell'ambito soggettivo di applicazione degli obblighi e delle misure in materia di trasparenza" (lett. *a*): si ricorda che già l'art. 24-bis, d.l. n. 90/2014, convertito, con modificazioni, dalla l. 114/2014, aveva modificato le disposizioni relative all'ambito soggettivo di applicazione del decreto 33, con particolare riferimento alle autorità indipendenti, sostituendo integralmente l'art. 11;

b) "riduzione e concentrazione degli oneri gravanti in capo alle amministrazioni pubbliche" ferme restando le previsioni in materia di verifica, controllo e sanzioni (lett. *c*);

c) razionalizzazione e precisazione degli obblighi di pubblicazione nel sito, al fine di evitare duplicazioni e consentire alle pp.aa. di assolvere gli obblighi attraverso la "pubblicità totale o parziale di banche dati detenute" (lett. *e*);

d) definizione dei diritti dei membri del Parlamento inerenti all'accesso ai documenti amministrativi e alla verifica dell'applicazione delle norme sulla trasparenza amministrativa. Tale diritto di accesso è circoscritto alle "esigenze connesse allo svolgimento dei compiti istituzionali" e può essere esercitato "nei limiti derivanti dal segreto o dal divieto di divulgazione", salvi i "casi di esclusione a tutela di interessi pubblici e privati" e fatti comunque salvi i poteri di controllo del Copasir (lett. *f*);

e) riconoscimento della "libertà di informazione" atttaverso il "diritto di accesso anche per via telematica di chiunque, indipendentemenre dalla titolarità di situazioni giuridicamente rilevanti, ai dati e ai documenti detenuti" dalle pp.aa. (lett. *h*). Con tale criterio di delega – frutto di un emendamento parlamentare presentato alla Camera e poi riformulato su proposta del relatore e sul quale la ministra Madia ha espresso parere favorevole – si introduce, in sostanza, un nuovo "diritto di accesso" ai dati e ai documenti detenuti dalle pp.aa., molto ampio e diverso non solo da quello *ex* l. n. 241/1990, ma anche da quello "civico" introdotto dal decreto 33 (il criterio di delega, infatti, lascia inaltetati gli obblighi di pubblicazione). Il nuovo diritto è introdotto "al fine di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse". Circa i limiti all'esercizio del dititto in questione, la disposizione fa "salvi i casi di segreto o di divieto di divulgazione previsti dall'ordinamento" e richiede il "rispetto dei limiti relativi alla tutela di interessi pubblici e ptivati".

Carta della cittadinanza digitale

f) L'art. 1 della legge, significativamente modificato al Senato e poi alla Camera, rubricato Carta della cittadinanza digitale (e non più Accelerazione e semplificazione nei servizi per i cittadini e le imprese), delega il Governo ad adottare decreti legislativi per disciplinare le modalità di erogazione dei servizi ai cittadini, assicurando la piena accessibilità *online* ai servizi, alle informazioni e ai documenti in possesso delle pp.aa., riducendo la necessità dell'accesso fisico agli uffici pubblici.

Di tale delega – che dovrà essere esercitata mediante modifiche al Cad – si riportano i criteri di maggior interesse per l'Autorità o sotto il profilo della protezione dei dati personali, in gran parte introdotti o rimodulati durante l'esame in Parlamento:

- accentuazione nella prospettiva del codice di settore del "diritto" dei cittadini all'accesso in modalità digitale ("anche" mediante l'utilizzo delle tecnologie dell'informazione e della comunicazione) ai dati, documenti, servizi di loro interesse; previsione al fine di garantire la semplificazione nell'"accesso ai servizi alla persona" (art. 1, comma 1, alinea);
- definizione di un "livello minimo" di sicurezza, qualità, accessibilità e tempestività dei servizi *online* delle amministrazioni, con locuzione che si direbbe evocativa dei "livelli essenziali delle prestazioni concernenti i diritti civili e sociali che devono essere garantiti su tutto il territorio nazionale", di cui all'art. 117, secondo comma, lettera *m*), Cost. (art. 1, comma 1, lett. *a*);
- previsione, in merito ai requisiti minimi o obiettivi della digitalizzazione delle amministrazioni, dell'accesso e riuso gratuito delle informazioni prodotte e detenute dalla pp.aa.; partecipazione telematica; piena disponibilità di sistemi di pagamento elettronico; "alfabetizzazione digitale"; partecipazione con modalità telematiche ai processi decisionali delle Istituzioni pubbliche; riduzione del divario digitale (lett. *c*);
- ridefinizione del sistema pubblico di connettività e razionalizzazione delle disposizioni vigenti in materia di identificazione, comunicazione e autorizzazione in rete nell'ambito del Sistema pubblico di identità digitale (Spid) promuovendo l'adesione delle pp.aa. e dei privati allo Spid (lett. *d*);
- promozione dell'elezione di un domicilio digitale da parte del cittadino (lett. *g*);
- semplificazione dell'accesso al sostegno della genitorialità corrispondente al profilo dei richiedenti, attraverso l'utilizzo del sito dell'Inps collegato con i siti delle amministrazioni regionali e locali, attivabile all'iscrizione anagrafica del figlio nato o adottato, secondo modalità e procedure che garantiscano la certezza e riservatezza dei dati (lett. *h*);
- ottimizzazione della spesa nei processi di digitalizzazione favorendo l'uso di *software open source* per il coordinamento e la collaborazione delle pp.aa. (lett. *i*);
- adeguamento alla disciplina europea in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche (lett. *p*);
- previsione del pagamento digitale ed elettronico, effettuato con qualsiasi modalità, quale mezzo principale per i pagamenti dovuti alla p.a. (lett. *q*);

Enti territoriali

4) il decreto-legge 19 giugno 2015, n. 78, convertito dalla l. 6 agosto 2015, n. 125, recante disposizioni urgenti in materia di enti territoriali, tra le cui disposizioni si segnala l'art. 10 in materia di Anagrafe nazionale della popolazione residente (Anpr) e di carta d'identità elettronica. La disposizione – modificando l'art. 62 del Cad – prevede che l'Anpr contenga anche l'archivio nazionale informatizzato dei registri di stato civile tenuti dai comuni e fornisca i dati ai fini della tenuta delle liste di leva; inoltre, l'Anpr assicura ai singoli comuni la disponibilità dei dati, degli atti e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite al sindaco e mette a disposizione dei comuni un sistema di controllo, gestione e interscambio, puntuale e massivo, di dati, servizi e transazioni necessario ai sistemi locali per lo svolgimento delle funzioni istituzionali di competenza comunale. Al fine dello svolgimento delle proprie funzioni, ad eccezione di quelle assicurate dall'Anpr e solo fino al completamento dell'Anagrafe nazionale, il comune può utilizzare i dati anagrafici eventualmente conservati localmente, costantemente alli-

neati con l'Anpr. In merito alla carta d'identità elettronica, nel ribadire che si tratta di una competenza riservata al Ministero dell'interno, si rinvia per l'attuazione ad un decreto del predetto Ministro, di concerto con il Ministro per la semplificazione e la pubblica amministtazione, sentito anche il Garante;

2

Misure urgenti in materia fallimentare civile e processuale civile

5) il decreto-legge 27 giugno 2015, n. 83, recante Misure urgenti in materia fallimentare, civile e processuale civile e di organizzazione e funzionamento dell'amministrazione giudiziaria, convertito dalla l. 6 agosto 2015, n. 132, contiene varie disposizioni di interesse, tra cui la previsione concernente il concordato preventivo, a mente della quale il commissario giudiziale fornisce ai creditori che ne fanno richiesta, le informazioni utili per la presentazione di proposte concorrenti, sulla base delle scritture contabili e fiscali obbligatorie del debitore, nonché ogni altra informazione rilevante in suo possesso, valutata la congruità della richiesta medesima e previa assunzione di opportuni obblighi di riservatezza (art. 3, comma 2). Un'altra disposizione prevede, inoltre, che – in relazione all'espropriazione forzata (art. 490 c.p.c.) – quando la legge dispone che di un atto esecutivo sia data pubblica notizia, deve essere inserito sul portale del Ministero della giustizia in un'area pubblica denominata "portale delle vendite pubbliche" un congruo ed esaustivo avviso (art. 13). La legge in parola – modificando l'art. 155-*ter* delle disp. att. del c.p.c – prevede altresì che le pp.aa. che gestiscono banche dati contenenti informazioni utili ai fini della ricerca con modalità telematiche dei beni da pignorare, mettano a disposizione degli ufficiali giudiziari i necessari accessi, con le modalità di cui all'art. 58 del Cad. Sino a quando non saranno definiti dall'AgID gli *standard* di comunicazione e le regole tecniche di cui al predetto art. 58 e, in ogni caso, quando l'amministrazione che gestisce la banca dati o il Ministero della giustizia non dispongano dei sistemi informatici per la cooperazione applicativa di cui all'art. 72, comma 1, lett. *e*), del medesimo Cad, l'accesso è consentito previa stipulazione di una convenzione finalizzata alla fruibilità informatica dei dati, sentito il Garante. Il Ministero della giustizia pubblica sul portale dei servizi telematici l'elenco delle banche dati per le quali è operativo l'accesso da parte dell'ufficiale giudiziario (art. 14);

Istruzione

6) la legge 13 luglio 2015, n. 107, recante Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti (cd. buona scuola) la quale presenta alcune disposizioni di interesse per l'Autorità delle quali si fornisce di seguito una breve disamina:

a) (*curriculum* dello studente e Portale unico dei dati dello studente). L'art. 1, comma 28, nel disciplinare il percorso formativo degli studenti, introduce il *curriculum* dello studente – che individua il "profilo" dello studente associandolo a una "identità digitale" – nel quale sono raccolti i dati relativi al percorso di studi, alle esperienze formative e alle competenze acquisite sia in ambito scolastico, sia extrascolastico che in alternanza scuola-lavoro, utili ai fini dell'orientamento e dell'accesso al mondo del lavoro. Premesso che è istituito il Portale unico dei dati della scuola (art. 1, comma 136), gestito dal Ministero dell'istruzione, dell'università e della ricerca (Miur), la legge prevede che tale portale renda "accessibili i dati del *curriculum*" dello studente, "condivisi con il Ministero da ciascuna istituzione scolastica" (art. 1, comma 138). L'originaria formulazione del disegno di legge lasciava spazio a dubbi interpretativi sui limiti e sulle condizioni con cui potesse avvenire la "pubblicazione" del *curriculum* dello studente e non precisava il ruolo del Garante nella "gestione" del portale da parte del Ministero (si prevedeva genericamente che l'Autorità fosse sentita, senza specificare però su quale atto o provvedimento del Ministero). In tale quadro si apprezza la modi-

fica intervenuta nel corso dei lavori parlamentari (cfr. art. 1, comma 28) con la previsione di un regolamento del Miur, da adottare sentito il Garante, per disciplinare le modalità di individuazione del profilo dello studente da associare ad un'identità digitale, le modalità di trattamento dei dati personali contenuti nel *curriculum* dello studente da parte di ciascuna istituzione scolastica, nonché le modalità di trasmissione al Ministero dei suddetti dati per renderli accessibili nel Portale unico dei dati della scuola, nonché i criteri e le modalità per la "mappatura del *curriculum*". Si rileva al riguardo che le disposizioni appena descritte pongono l'esigenza di un coordinamento con le previsioni del Codice in materia di istruzione, e in particolare con l'art. 96, il quale prevede che le scuole possano comunicare a terzi o diffondere dati personali (non aventi natura sensibile) degli studenti per finalità di orientamento, formazione o inserimento nel mondo del lavoro, ma solo a richiesta dell'interessato e con vincolo di finalità. La legge prevede poi (art. 1, comma 137) che il Ministero, in conformità con quanto disposto dall'art. 68, comma 3, del Cad e in applicazione del d.lgs. 24 gennaio 2006, n. 36, garantisca stabilmente l'accesso e la riutilizzabilità dei dati pubblici del sistema nazionale di istruzione e formazione, pubblicando in formato aperto i dati relativi ai bilanci delle scuole, i dati pubblici afferenti il Sistema nazionale di valutazione, l'Anagrafe dell'edilizia scolastica, i provvedimenti di incarico di docenza, i piani dell'offerta formativa, i dati dell'Osservatorio tecnologico, i materiali e le opere autoprodotte dagli istituti scolastici e rilasciati in formato aperto secondo le modalità di cui all'art. 15, d.l. n. 112/2008, convertito dalla l. n. 133/2008. Al riguardo si sottolinea che la disposizione prevede espressamente che l'accesso e la riutilizzabilità dei dati sia assicurata "in applicazione" del d.lgs. n. 36/2006, il quale, com'è noto, in attuazione della direttiva 2013/37/UE è stato recentemente modificato dal d.lgs. n. 102/2015 (sul cui schema il Garante ha reso parere a richiesta del Governo, cfr. par. 3.4.2) e prevede, in ogni caso, la salvaguardia della normativa in materia di protezione dei dati personali (art. 4, comma 1, lett. *a*).

b) (Alternanza scuola-lavoro). È stata integrata la disciplina volta ad incremenrare le opportunità di lavoro degli studenti, mediante l'istituzione, a decorrere dall'anno scolastico 2015/2016, presso le camere di commercio del "registro nazionale per l'alternanza scuola-lavoro" (art. 1, comma 41). Il registro (la norma non specifica da quale Amministrazione debba essere istituito e con quale atto) consta delle seguenti componenti: a) un'area aperta e consultabile gratuitamente in cui sono visibili le imprese e gli enti pubblici e privati disponibili a svolgere i percorsi di alternanza, con l'indicazione, per ciascuna impresa, del numero massimo degli studenti ammissibili; b) una sezione speciale del registro delle imprese di cui all'art. 2188 c.c., a cui devono essere iscritte le imprese per l'alternanza scuola-lavoro; tale sezione consente la condivisione, nel rispetto della normativa sulla tutela dei dati personali, delle informazioni relative all'anagrafica, all'attività svolta, ai soci e agli altri collaboratori, al fatturato, al patrimonio netto, al sito internet e ai rapporti con gli altri operatori della filiera delle imprese che attivano percorsi di alternanza.

c) (Piano nazionale per la scuola digitale). Sul piano applicativo, si richiama l'attenzione sull'adozione da parte del Miur del Piano nazionale per la scuola digitale, destinato a perseguire, fra gli altri obiettivi, anche l'ado-

zione di strumenti organizzativi e tecnologici per favorire la trasparenza e la condivisione di dati, nonché lo scambio di informazioni tra dirigenti, docenti e studenti e tra istituzioni scolastiche ed educative e articolazioni amministrative del Ministero (art. 1, commi 56 e 58, lett. *c*).

d) (*Bonus*-scuola). Si segnalano infine le disposizioni che prevedono un credito d'imposta per le erogazioni liberali in denaro destinate agli investimenti in favore degli istituti del sistema nazionale di istruzione, per la realizzazione di nuove strutture scolastiche, la manutenzione e il potenziamento di quelle esistenti e per il sostegno a interventi che migliorino l'occupabilità degli studenti (art. 1, commi 145-150). Di interesse è il comma 149 dell'articolo, in base al quale i soggetti beneficiari delle erogazioni liberali provvedono a dare pubblica comunicazione dell'ammontare delle erogazioni liberali ricevute nel mese di riferimento, nonché della destinazione e dell'utilizzo delle erogazioni stesse tramite il proprio sito web istituzionale e sul portale telematico del Ministero, nel rispetto delle disposizioni del Codice. La disposizione non sembra fare riferimento a dati personali (segnatamente dei soggetti che hanno erogato la liberalità), ma solo all'ammontare delle erogazioni liberali ricevute nonché alla loro destinazione e utilizzo;

7) la legge 9 luglio 2015, n. 114, recante Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea (legge di delegazione europea 2014). Fra gli atti ai quali il Governo è chiamato a dare attuazione rilevano, per gli aspetti di protezione dei dati personali:

Recepimento direttive europee

a) le direttive 2010/53/UE e 2012/25/UE, relative alle norme di qualità e sicurezza ed alle procedure informative per lo scambio tra Stati membri di organi umani destinati ai trapianti. Una prima esecuzione alla direttiva del 2010 è stata assicurata dalla l. 24 dicembre 2012, n. 228, in attuazione della quale il Ministero della salute ha adottato un decreto per la disciplina dei prelievi e trapianti di organi e tessuti, ivi compreso il profilo dello scambio di organi a livello europeo ai sensi della direttiva del 2012, sul cui schema il Garante ha reso parere in data 28 maggio 2015 (cfr. par. 3.4.1);

b) la direttiva 2015/413/UE, intesa ad agevolare lo scambio transfrontaliero di informazioni sulle infrazioni in materia di sicurezza stradale, che sostituisce la direttiva 2011/82/UE, annullata con la sentenza della CGUE, Grande Sezione, del 6 maggio 2014 per vizi riguardanti il fondamento giuridico (quello appropriato è l'art. 91, paragrafo 1, lettera *c*), TFUE). Si rammenta che in attuazione della precedente direttiva il Governo ha emanato il d.lgs. 4 marzo 2014, n. 37, sul cui schema il Garante ha reso parere all'esito di un tavolo tecnico, istituito presso la Presidenza del Consiglio dei ministri, cui aveva fornito il proprio contributo anche il Garante per quanto riguarda gli aspetti di protezione dei dati personali (parere 9 gennaio 2014, n. 2, doc. web n. 2904320);

c) la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione, che sostituisce la decisione quadro 2005/222/GAI del Consiglio e la direttiva 2014/107/UE recante modifica della direttiva 2011/16/UE per quanto riguarda lo scambio automatico obbligatorio di informazioni nel settore fiscale. Infine, gli artt. 19 e 20 della legge di delegazione autorizzano il Governo a dare attuazione a due decisioni quadro in materia di scambi fra gli Stati membri di informazioni estratte dal casellario giudiziario e istituzione del sistema europeo di informazione sui casellari giudiziari (ECRIS) (decisioni 2009/315/GAI e 2009/316/GAI);

FATCA

8) la legge 18 giugno 2015, n. 95, recante la ratifica ed esecuzione dell'Accordo tra il Governo della Repubblica italiana e il Governo degli Stati Uniti d'America finalizzato a migliorare la *compliance* fiscale internazionale e ad applicare la normativa FATCA (*Foreign Account Tax Compliance Act*), con Allegati, fatto a Roma il 10 gennaio 2014, nonché disposizioni concernenti gli adempimenti delle istituzioni finanziarie italiane ai fini dell'attuazione dello scambio automatico di informazioni derivanti dal predetto Accordo e da accordi tra l'Italia e altri Stati esteri;

Contrasto del terrorismo

9) il decreto-legge 18 febbraio 2015, n. 7, convertito dalla l. 17 aprile 2015, n. 43, recante misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, di cui si segnalano diverse disposizioni di interesse in relazione alle quali, peraltro, il Garante ha avuto modo di evidenziare alcune criticità in sede di audizione presso le Commissioni riunite giustizia e difesa della Camera nel corso dei lavori per la conversione del provvedimento d'urgenza (cfr. par. 3.2). Rileva, innanzitutto l'art. 7 che riscrive l'art. 53 del Codice, definendo quali siano i trattamenti effettuati per finalità di polizia ed estendendo l'esonero dall'applicazione di alcune disposizioni del Codice – laddove ne ricorrano i presupposti – anche ai trattamenti di dati personali previsti, non solo da disposizioni di legge, ma anche da disposizioni regolamentari, nonché individuati dal decreto del Ministro dell'interno. Al riguardo il Garante in sede di audizione – dopo aver "contestualizzato" il decreto d'urgenza nel clima di allarme creatosi a seguito delle minacce terroristiche – ha osservato che l'art. 53 all'epoca vigente, nel prevedere un regime agevolato (che esime da alcuni obblighi come informativa, notificazione ecc.) per i soli trattamenti specificamente previsti da espressa disposizione legislativa, poteva probabilmente aver rallentato, in alcuni casi, l''esigenza di continuo e celere adeguamento degli strumenti investigativi all'evoluzione tecnologica. L'Autorità ha ritenuto, perciò, comprensibile la proposta di includere, tra le fonti idonee a legittimare la raccolta di dati, oltre alla legge ordinaria, anche le norme regolamentari e lo specifico decreto del Ministro. Del resto, dovendo queste nuove fonti riflettere specifiche attribuzioni della polizia, l'ambito di discrezionalità del Governo o dello stesso Ministro sarà indubbiamente limitato in ragione della natura dell'azione dell'autorità di pubblica sicurezza idonea a incidere su diritti fondamentali e pertanto rigidamente disciplinata dalla legge. Il Garante inoltre ha osservato che questo nuovo regime previsto per la polizia – che in certa misura lo avvicina, pur con maggiori vincoli, a quello sancito per fini di giustizia – appare compatibile con il nuovo quadro giuridico europeo, che progressivamente assimila questi due settori (ivi inclusa la polizia di prevenzione). L'Autorità ha concluso sottolineando l'esigenza di garantire l'equilibrio complessivo del nuovo sistema fornendo la più ampia disponibilità, in particolare mediante il necessario parere ai sensi dell'art. 154, comma 4, del Codice sui menzionati regolamenti e decreto.

Di interesse sono poi altre disposizioni in materia di contrasto del proselitismo *online*. In proposito – sempre nella predetta audizione – il Garante ha ritenuto utile un'occasione di confronto nell'attuazione della disciplina dell'inibizione, su ordine dell'autorità giudiziaria, dell'accesso a siti filo-terroristi (inclusi cioè nella *black list* stilata dalla polizia postale), secondo modalità e soluzioni tecniche individuate dal d.m. del 2007 sulla pedopornografia (art. 2, commi 2 e 3). Come pure nell'attuazione (nonostante non sia espressamente previsto un decreto o altro provvedimento) della diversa previsione di cui all'art. 2, comma 4, sulla rimozione selettiva dei contenuti illeciti pubblicati su siti utilizzati da terroristi, che sembrerebbe includere – con una significativa innovazione rispetto al codice del commercio elettronico – anche i *social network* (luoghi nei quali si svolge prevalentemente l'azione di proselitismo e apologia). L'equilibrio di questa disciplina – che va salvaguardato anche ai

fini dell'art. 21 Cost. – si fonda essenzialmente su due aspetti. In primo luogo, sulla limitazione della rimozione ai soli contenuti accessibili al pubblico, e non alle comunicazioni private. In secondo luogo, sul sistema di segnalazione e rimozione (*notice and take down*: il solo compatibile con la disciplina europea), che esclude cioè ogni preventiva censura, da parte del *provider*, dei contenuti diffusi in rete, ammettendone la rimozione selettiva solo su specifico ordine dell'autorità giudiziaria. Il Garante potrà, anche in questo caso, fornire un contributo, in fase di attuazione, al fine di garantire la conformità di tali misure con il diritto alla riservatezza degli utenti della rete.

Di interesse sono anche le disposizioni in tema di *data retention.*

Da un lato, il comma 1-*quater* del medesimo art. 2, integrando l'art. 226 delle norme di attuazione del c.p.p in tema di intercettazioni preventive (comma 3-*bis*), stabilisce che, in deroga a quanto previsto in via generale sull'attività di intercettazione, il procuratore può autorizzare, per un periodo non superiore a ventiquattro mesi, la conservazione dei dati acquisiti, anche relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, quando gli stessi sono indispensabili per la prosecuzione dell'attività finalizzata alla prevenzione dei pertinenti gravi delitti.

Dall'altro, con disposizione *extra-ordinem*, per agevolare le indagini su reati gravi riconducibili, in particolare, alla criminalità organizzata e al terrorismo, il decreto ha disciplinato la conservazione dei dati di traffico telefonico e telematico in deroga a quanto previsto dall'art. 132 del Codice (art. 4-*bis*). La disposizione – in base alle modifiche apportatevi poi dal d.l. 30 dicembre 2015, n. 210, cd. milleproroghe – prevede che per finalità di accertamento e repressione dei predetti reati, i dati relativi al traffico telefonico o telematico, esclusi comunque i contenuti della comunicazione, detenuti dagli operatori dei servizi di telecomunicazione alla data di entrata in vigore della legge di conversione del decreto, nonché quelli relativi al traffico telefonico o telematico effettuato successivamente a tale data, e i dati relativi alle chiamate senza risposta effettuate a decorrere dalla data di entrata in vigore della legge di conversione del decreto, trattati temporaneamente da parte dei fornitori di servizi, siano conservati fino al 30 giugno 2017 (l'originario termine era stato fissato al 31 dicembre 2016).

Infine, allo scopo di assicurare al Ministero dell'interno l'immediata raccolta delle informazioni in materia di armi, munizioni e sostanze esplodenti, le questure territorialmente competenti potranno ricevere le informazioni e i dati previsti, avvalendosi di mezzi informatici o telematici, secondo modalità e tempi stabiliti con decreto del Ministro dell'interno, sentito il Garante (art. 3, comma 3-*bis*).

2.1.2. I decreti legislativi

Nel 2015 sono stati approvati numerosi decreti legislativi che hanno riflessi in materia di protezione dei dati personali, fra i quali si menzionano in particolare:

1) il decreto legislativo 14 settembre 2015, n. 151, – adottato in attuazione della l. 14 settembre 2014, n. 183 – nell'ambito del quale è di particolare rilievo l'art. 23 che apporta significative modifiche all'art. 4 dello Statuto dei lavoratori (l. n. 300/ 1970). L'articolo dà attuazione al criterio di delega previsto all'art. 1, comma 7, lett. *f*), della l. n. 183/ 2014, che demanda al Governo "la revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore". L'inciso "sugli impianti e sugli strumenti di lavoro" è stato aggiunto in seconda lettura, dal momento che il testo approvato dal Senato riferiva l'oggetto della delega, più gene-

ricamente, alla revisione della disciplina "dei controlli a distanza". Alla luce di tale precisazione normativa, è forse legittimo il dubbio che il decreto sia intervenuto su un ambito più ampio rispetto all'oggetto della delega.

Le principali innovazioni apportate all'art. 4 dello Statuto riguardano:

a) l'espressa legittimazione dei controlli cd. difensivi per la tutela del patrimonio aziendale (che la giurisprudenza, sia pur con qualche limite, già ammetteva), la cui discipliua è ricondotta alla procedura generale coucertativo-autorizzativa;

b) il mutamento della procedura concertativa;

c) l'esclusione dalla procedura concertativo-autorizzativa dei controlli realizzati mediante gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e gli strumenti di registrazione degli accessi e delle presenze" (ad es., i lettori *badge*). Riguardo a quest'ultimo aspetto, il Ministero del lavoro – con un comunicato 18 giugno 2015 – ha chiarito che l'esonero dalla procedura autorizzativa non si applica nel momento in cui lo strumento viene modificato (ad es., con l'aggiunta di *software* di localizzazione o di filtraggio). In tali casi, infatti, come ha specificato il Ministero, "da strumento che serve al lavoratore per rendere la prestazione, il pc, il *tablet* o il cellulare divengono strumenti che servono al datore per controllarne la prestazione";

d) la possibilità di utilizzare i dati raccolti mediante i suddetti controlli (a distanza o "sugli strumenti di lavoro") "a tutti i fini connessi al rapporto di lavoro", purché sia data al lavoratore "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto" dal Codice. Quest'ultimo profilo – che, peraltro, sembra collocarsi "al limire" del criterio di delega, il quale, almeno formalmente, non appare comprensivo della fase, successiva al controllo, dell'utilizzazione delle informazioni così ottenute nell'esercizio di poreri datoriali (direttivo, disciplinare) diversi dal potere di controllo – è di particolare delicatezza anche perché sembra rappresentare un'innovazione non irrilevante rispetto all'indirizzo giurisprudenziale che, ad es., ha escluso l'utilizzabilità dei dari ottenuti con controlli difensivi (già ammessi dalla giurisprudenza, come detto), per provare l'inadempimento contrattuale del lavoratore (cfr. Cass. n. 16622/2012).

Nel complesso, si ttarta, evidentemente, di un'estensione delle possibilità di utilizzo degli strumenti di controllo e dei dati acquisiri notevole ma non certo illimitata che troverà i suoi limiti non solo nelle finalità già indicate dalla norma per la predisposizione dei controlli (arr. 4, comma 1), ma anche nei princìpi previsti dalla normativa, anche sovranazionale (diretriva 95/46/CE e, da ultimo, la raccomandazione del Consiglio d'Europa del 1° aprile 2015), a garanzia dei diritti fondamentali degli interessati rispetto al trartamento dei loro dati personali.

Ciò – come è stato precisato dal Garanre nell'audizione tenuta innanzi alle Commissioni lavoro di Camera e Senato nel mese di luglio (cfr. par. 3.2) – non solo esclude l'ammissibilità di controlli massivi, ma impone comunque una gradualità nell'ampiezza e tipologia del moniroraggio, in modo da rendere assolutamente residuali i controlli più invasivi, legirtimandoli solo a fronte della rilevazione di specifiche anomalie e comunque all'esiro dell'esperimento di misure preventive meno limirative dei diritri dei lavoratori. In questa prospettiva – riprendendo anche in questo caso quanto già segnalaro dal Garante al Parlamento nella citara audizione – assai utile può essere l'adozione di una soluzione di *privacy by design*, ovvero la progettazione degli stessi strumenti in modo da minimizzare, fino ad escludere, il

rischio di controlli invasivi o comunque di incisive limitazioni della riservatezza di chi a quei controlli possa essere sottoposto. È significativo, del resto, che tali soluzioni siano valorizzate non solo dalla già citata raccomandazione, ma anche nel regolamento UE sulla protezione dati la cui pubblicazione è prevista sulla GUUE del 4 maggio 2016.

In conclusione, il principale argine a un utilizzo pervasivo dei controlli sul lavoro sarà nella conformità alle norme del Codice e in questo senso molto utili saranno i princìpi generali che sinora hanno consentito al Garante di adeguare la disciplina del 1970 (cui lo stesso Codice rinvia all'art. 113) a una realtà così fortemente mutata (necessità, correttezza, determinatezza, legittimità ed esplicitazione del fine perseguito dal trattamento – che dovrebbe, quest'ultimo, come detto, concorrere a un'interpretazione "adeguatrice" del nuovo art. 4 –, pertinenza e non eccedenza dei dati trattati, ma anche, più nello specifico, divieto di profilazione).

Vi sono poi altre disposizioni di interesse per l'Autorità, introdotte in attuazione di diversi princìpi di delega.

L'articolo 8, integrando l'art. 9, l. 12 marzo 1999, n. 68, con il comma 6-*bis*, istituisce all'interno della banca dati delle politiche attive e passive di cui all'art. 8, d.l. 28 giugno 2013, n. 76, convertito dalla l. n. 99/2013, la banca dati del collocamento mirato (riservato ai lavoratori disabili), al fine di razionalizzare la raccolta sistematica dei dati disponibili, di semplificare gli adempimenti e di rafforzare i controlli. La nuova banca dati è destinata a raccogliere le informazioni, per molta parte di natura sensibile, concernenti i datori di lavoro pubblici e privati e i lavoratori disabili interessati. La norma disciplina l'alimentazione della banca dati da parte dei datori di lavoro e degli organi o uffici competenti, come ad esempio l'Inps, l'Inail (che alimenta la banca dati con le informazioni relative agli interventi in materia di reinserimento e di integrazione lavorativa delle persone con disabilità da lavoro) o le regioni e le province autonome di Trento e Bolzano (il cui debito informativo riguarda le informazioni relative agli incentivi e alle agevolazioni in materia di collocamento delle persone con disabilità erogate sulla base di disposizioni regionali). Le informazioni della banca dati sono rese disponibili alle regioni e province autonome di Trento e Bolzano e agli altri enti pubblici responsabili del collocamento mirato con riferimento al proprio ambito territoriale di competenza, nonché all'Inail ai fini della realizzazione dei progetti personalizzati in materia di reinserimento e di integrazione lavorativa delle persone con disabilità da lavoro. Sarà importante il contributo che il Garante potrà fornire al Ministero in sede di parere sullo schema di decreto al fine di assicurare garanzie adeguate ai dati sensibili che saranno così trattati.

Altra disposizione di interesse è l'art. 17 (Banche dati in mareria di politiche del lavoro) che intende dare concreta attuazione alla menzionata banca dati delle politiche attive e passive e in tal senso con uno o più decreti del Ministro del lavoro, di concerto con il Ministro per la semplificazione e la pubblica amministrazione e il Ministro dell'interno, dovranno essere individuate in dettaglio le informazioni che vi devono confluire (già delineate, per "categorie", nell'art. 8, comma 2, d.l. n. 76/2013, ovvero le informazioni concernenti i soggetti da collocare nel mercato del lavoro, quelle relative agli incentivi, ai datori di lavoro pubblici e privati, ai collaboratori e ai lavoratori autonomi, agli studenti e ai cittadini stranieri regolarmente soggiornanti in Italia per motivi di lavoro), i soggetti che possono inserire, aggiornare e consultare le informazioni, nonché le modalità di inserimento, aggiornamento e consultazione, nel rispetto delle disposizioni del Codice. Dal momento che tali dati possono anche rivestire natura sensibile, anche in questo caso il Garante potrà fornire indicazioni utili in punto di garanzie per gli interessati in occasione del parere

da rendere ai sensi dell'art. 154, comma 4, del Codice. Infine, il comma 3 dell'articolo precisa che le disposizioni in questione sostituiscono la comunicazione al Garante di cui all'arr. 39, comma 1, lett. *a*), del Codice. La disposizione normativa sembra ultronea, dal momenro che la procedura cui si fa riferimenro (comunicazione al Garante della necessità di un flusso informativo fra soggetti pubblici) è necessaria nei casi nei quali il rrarramento non abbia copertura normativa (circostanza che non ricorre nella fattispecie).

L'articolo 17 istituisce altresì nella già citata banca dati delle politiche artive e passive una sezione denominata "fascicolo dell'azienda" – contenente tutte le informazioni sui datori di lavoro ricavabili dalle comunicazioni obbligatorie – e che rileva ai nostri fini solo in quanto concerna imprenditori individuali, dal momenro che le persone giuridiche non sono più soggetti di diritto ai sensi della normativa in materia di protezione dei dati personali.

2) Il decreto legislativo 14 settembre 2015, n. 150, contiene importanti disposizioni in materia di politiche attive per il lavoro, anche al fine di semplificare diversi adempimenti amministrativi e razionalizzare il sistema. Innanzitutto istituisce la rete nazionale dei servizi per le politiche del lavoro cosrituita dai seguenri soggetti, pubblici o privati: a) l'Agenzia nazionale per le politiche attive del lavoro (Anpal), istituita a decorrere dal 1° gennaio 2016, dall'art. 4 dello sresso decteto; b) le strutture regionali per le politiche artive del lavoro (art. 11); c) l'Inps, in relazione alle competenze in materia di incentivi e strumenti a sostegno del reddito; d) l'Inail, in relazione alle competenze in materia di reinserimento e di integrazione lavorativa delle persone con disabilità da lavoro; e) le Agenzie per il lavoro, di cui all'art. 4, d.lgs. 10 settembre 2003, n. 276, e gli altri soggetti autorizzati all'attività di intermediazione (art. 12); f) l'Istituto per lo sviluppo della formazione professionale dei lavoratori (Isfol) e Italia Lavoro S.p.A.; g) il sistema delle camere di commercio, le università e gli istituti di scuola secondaria di secondo grado. La rete dei servizi per le politiche del lavoro promuove l'effertività dei diritti al lavoro, alla formazione ed all'elevazione professionale previsti dalla Costituzione ed il diritto di ogni individuo ad accedere a servizi di collocamenro gratuito, di cui all'art. 29 della Carta dei diritti fondamentali dell'Unione europea. Al Ministero spetta il potere di indirizzo e vigilanza sull'Anpal, che si esprime anche mediante l'adozione del parere preventivo su determinati atti del nuovo organismo, nonché le competenze in mareria di verifica e controllo del rispetto dei livelli essenziali delle prestazioni (art. 2).

Particolare rilevanza sotto il profilo della prorezione dei dati personali è l'art. 13 in base al quale, in attesa della realizzazione di un sistema informativo unico, l'Anpal realizza, in cooperazione con il Ministero, le regioni, le province autonome di Trenro e Bolzano, l'Inps e l'Isfol, valorizzando e riutilizzando le componenti informatizzate realizzate dalle predette amministrazioni, il sistema informativo unitario delle politiche del lavoro, che si compone del nodo di coordinamento nazionale e dei nodi di coordinamento regionali, nonché il portale unico per la regisrrazione alla Rete nazionale dei servizi per le politiche del lavoro. Costituiscono elementi del predetto sistema informativo unitario: a) il sistema informativo dei percettori di ammortizzatori sociali (art. 4, comma 35, l. n. 92/2012); b) l'archivio informatizzato delle comunicazioni obbligatorie (art. 6, d.lgs. n. 297/2002); c) i dati relativi alla gestione dei servizi per il lavoro e delle politiche attive del lavoro, ivi incluse la scheda anagrafica e professionale; d) il sistema informativo della formazione professionale, di cui all'art. 15 del decrero stesso. Il medesimo art. 13, al comma 3, precisa che il modello di scheda anagrafica e professionale dei lavoratori, di cui all'art. 1-*bis*, d.lgs. n. 181/2000, sia definito dall'Anpal, unitamente alle modalità di interconnessione tra i centri per l'impiego e il sistema informativo unitario delle politi-

che del lavoro. Inoltre, allo scopo di certificare i percorsi formativi seguiti e le esperienze lavorative effettuate, l'Anpal definisce apposite modalità di lettura delle informazioni contenute nel sistema informativo a favore di altri soggetti interessati, nel rispetto del diritto alla protezione dei dati personali (comma 5) e per monitorare gli esiti occupazionali dei giovani in uscita da percorsi di istruzione e formazione, stipula una convenzione con il Miur per lo scambio reciproco dei dati individuali e dei relativi risultati statistici.

In base all'art. 14 (Fascicolo elettronico del lavoratore e coordinamento dei sistemi informativi) le informazioni del sistema informativo unitario delle politiche del lavoro costituiscono il patrimonio informativo comune del Ministero del lavoro e delle politiche sociali, dell'Inps, dell'Inail, dell'Isfol, delle regioni e province autonome, nonché dei centri per l'impiego, per lo svolgimento dei rispettivi compiti istituzionali. Esse costituiscono, inoltre, la base informativa per la formazione e il rilascio del fascicolo elettronico del lavoratore, contenente le informazioni relative ai percorsi educativi e formativi, ai periodi lavorativi, alla fruizione di provvidenze pubbliche e ai versamenti contributivi ai fini della fruizione di ammortizzatori sociali. Il fascicolo è liberamente accessibile, a titolo gratuito, mediante metodi di lettura telematica, da parte dei singoli soggetti interessati (comma 1). Il Ministero del lavoro accede alla banca dati istituita presso l'Anpal ai sensi dell'art. 13 al fine dello svolgimento dei compiti istituzionali, nonché ai fini statistici e del monitoraggio sulle politiche attive e passive del lavoro e sulle attività svolte dall'Anpal (comma 3).

Il quadro normativo descritto – unitamente all'art. 17 del decreto n. 151 – attua i criteri di delega volti alla telematizzazione degli adempimenti amministrativi funzionali alla gestione del rapporto di lavoro e all'informatizzazione delle politiche del lavoro. Il tema è di grande attualità e di estrema importanza per il Garante in ragione delle implicazioni che possono derivare dal trattamento di dati – anche sensibili – nell'ambito di grandi banche dati pubbliche.

Non v'è dubbio che le disposizioni in parola potranno consentire una migliore gestione delle politiche attive per il lavoro semplificando, altresì, diversi adempimenti amministrativi. Tuttavia – come è stato sottolineato dal Garante nell'audizione in Parlamento (cfr. par. 3.2) – i dati contenuti in questi fascicoli e nei sistemi informativi che li alimentano devono essere adeguatamente protetti, al fine di scongiurare accessi abusivi lesivi tanto della riservatezza del lavoratore, quanto dell'interesse pubblico alla corretta gestione delle politiche del lavoro.

L'asimmetria che ha caratterizzato, sinora, il rapporto tra processo di informatizzazione delle pp.aa. e sicurezza dei dati è uno dei fattori principali della vulnerabilità dei nostri sistemi informativi. È dunque essenziale che le banche dati di nuova costituzione e anche soltanto la loro interconnessione siano realizzate nel rispetto dei requisiti di sicurezza previsti dal Codice e che, per quanto possibile, la loro vulnerabilità sia contrastata riducendo "la superficie d'attacco". In questo senso, ogniqualvolta le finalità siano ugualmente perseguibili con dati anonimi, dovrebbe evitarsi l'utilizzo di dati identificativi: circostanza che non sembra, invece, adeguatamente prevista per tutti i flussi informativi disciplinati dai descritti artt. 13 e 14.

Su tale aspetto il Garante ha insistito in sede di audizione, specie con riferimento allo scambio di dati individuali (oltre ai relativi risultati statistici) tra il Miur e l'Anpal (peraltro in base a una mera convenzione tra i due enti), per mere finalità di monitoraggio degli esiti occupazionali dei giovani in uscita da percorsi di istruzione e formazione (art. 13, comma 6), auspicando che si prevedesse, fra le "pre-condizioni" del trattamento, almeno la documentata indispensabilità dell'utilizzo di dati non anonimi. Analoga previsione l'Autorità ha auspicato in merito all'art. 14, comma 3, relativamente all'accesso per fini statistici e di monitoraggio delle politi-

che attive e passive del lavoro, da parte del Ministero del lavoro, al sistema informativo unico delle politiche del lavoro.

In entrambi i casi le disposizioni non sono state perfezionate nel senso auspicato.

Quanto alla consultabilità delle informazioni, l'Autorità ha sottolineato l'opportunità che fosse, almeno in certa misura, limitata o quantomeno precisata con criteri soggettivi di accesso proporzionali alle effettive esigenze perseguite di volta in volta. Nella formulazione, confermata, della norma, invece, si prevede genericamente che le informazioni del sistema informativo unico per le politiche del lavoro costituiscano il "patrimonio informativo comune", per lo svolgimento dei rispettivi fini istituzionali, del Ministero del lavoro, dell'Anpal, dell'Isfol, dell'Inps, dell'Inail, delle regioni e proviiice autonome, nonché dei centri per l'impiego.

Il Garante ha altresì valutato generico l'att. 13, comma 5, a mente del quale la lettura dei dati contenuti nel sistema informativo unico delle politiche del lavoro può essere consentita da Anpal a non meglio precisati "altri soggetti interessati" sia pure "nel rispetto del diritto alla protezione dei dati personali". L'Autorità ha altresì espresso perplessità sul dettato dell'art. 16, comma, 2, ove avrebbero merirato analoga precisazione, in chiave "selettiva", i limiti che pur dovrebbero inconrrare il Ministero e l'Isfol nell'accesso, per fini di monitoraggio e valutazione, a "tutti i dati gestionali trattati dall'Anpal" e, rispettivamente, al sistema informativo unico delle politiche del lavoro.

Una considerazione merita l'art. 14 in relazione ai dati censiti nel nuovo sistema costituenti l'oggetto del fascicolo elettronico del lavoratore, "liberamente accessibile", *online*, da parte dei "singoli soggetti interessati". Anche in tale norma sarebbe stato opportuno – come ha rilevato il Garante nell'audizione – chiarire meglio i criteri di legittimazione soggettiva (e oggettiva) all'accesso, ovvero chi effettivamente possa consultare quelle informazioni (alcune verosimilmente anche di caratrere sensibile), con quale grado di "invasività" e con quali garanzie per la sicurezza dei dati e dei sistemi stessi.

In tale quadro normativo – non del tutto rassicurante sotto il profilo della protezione dei dirirti fondamentali degli interessati – assume peculiare importanza il ruolo che il Garante potrà svolgere in occasione dei pareri da rendere sugli schemi di provvedimento previsti in attuazione delle norme primarie. Ed è importante che ciò avvenga rispetto a tutti i provvedimenti di attuazione aventi impatto sulla protezione dei dati che saranno adottati (auspicabilmente anche dal Ministero, pur in mancanza di un'espressa previsione, che pure sarebbe stata opportuna) ivi comprese le determinazioni dell'Anpal (art. 13, commi 1, 3 e 5; art. 15, comma 1, rispetto al sistema informativo della formazione professionale in relazione al quale l'Anpal deve definire le modalità e gli *standard* di conferimento dei dati da parte dei soggetti che vi partecipano, informazioni che saranno messe a disposizione delle regioni), le convenzioni tra le amministrazioni interessate (art. 13, comma 6, e art. 14, comma 6), e le decisioni del citato Comitato (art. 14, comma 4), in relazione ai quali l'Autorità assicura sin d'ora la consueta collaborazione istituzionale.

Infine, di interesse è anche il dettato dell'art. 19 nella parte in cui – disciplinando il trattamento dei dati dei soggetti disoccupati in cerca di impiego – prevede che "sulla base delle informazioni fornite in sede di registrazione, gli utenti dei servizi per l'impiego vengono assegnati ad una classe di profilazione allo scopo di valutarne il livello di occupabilità, secondo una procedura automatizzata di elaborazione dei dati in linea con i migliori *standard* internazionali". La disposizione fa rifetimento ad un trattamento di dati automatizzato volto a definire il profilo dell'interessato e, sotto questo aspetto, pone l'esigenza di un coordinamento con quanto previsto dal Codice in termini di garanzie per l'interessato (artt. 14, comma 2, e 37, comma 1,

lett. *d*), del Codice, rispettivamente, sul diritto di opporsi al trattamento automatizzato e sull'obbligo di previa notificazione al Garante).

3) il decreto legislativo 23 aprile 2015, n. 54, recante l'attuazione della decisione quadro 2006/960/GAI del Consiglio del 18 dicembre 2006 relativa alla semplificazione dello scambio di informazioni e *intelligence* tra le Autorità degli Stati membri dell'Unione europea. Il decreto reca disposizioni a protezione dei dati personali, peraltro in linea con quanto previsto per altri scambi informativi (cfr. d.P.R. recante il regolamento di attuazione della l. 30 giugno 2009, n. 85, concernente l'istituzione della banca dati nazionale del dna e del laboratorio centrale per la banca dati nazionale del dna, sul cui schema il Garante ha reso a suo tempo parere) ed individua nel Garante l'autorità nazionale di controllo sui trattamenti dei dati. Nel corso dei lavori preparatori, l'Autorità ha partecipato ad una riunione tenutasi presso la Presidenza del Consiglio dei ministri, rappresentando alcune criticità sullo schema del decreto, fra le quali, in particolare, la locuzione adoperata per individuare i reati rispetto ai quali è consentito lo scambio informativo a fini di *intelligence* che, per la sua genericità, rischia di creare difficoltà applicative (cioè reati "commessi per realizzare il furto di identità relativo a dati personali") (cfr. par. 3.4.2).

4) il decreto legislativo 18 maggio 2015, n. 102, di recepimento della direttiva 2013/37/UE del 26 giugno 2013, che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico, adottato ai sensi della l. 7 ottobre 2014, n. 154 e recante modifiche al d.lgs. 24 gennaio 2006, n. 36 di attuazione della precedente direttiva. La nuova direttiva 2013/37/UE – nello stabilire in modo chiaro l'obbligo per gli Stati membri di rendere riutilizzabili tutti i documenti, a meno che l'accesso sia limitato o escluso ai sensi delle disposizioni nazionali sull'accesso ai documenti e fatte salve le altre eccezioni stabilite nella nuova direttiva – conferma il principio, da ritenersi ormai consolidato in ambito europeo, in base al quale il riutilizzo dei documenti non deve pregiudicare il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali fissato dalle disposizioni di diritto europeo e nazionale in materia (art. 1, par. 4, direttiva 2003/98/CE, come modificato dall'art. 1, par. 1), lett. *c*), direttiva 2013/37/UE). In particolare, le nuove disposizioni della direttiva introducono specifiche eccezioni al riutilizzo fondare sui princìpi di protezione dei dati personali, prevedendo che una serie di documenti del settore pubblico contenenti tale tipologia di informazioni siano sottratti al riuso anche qualora siano liberamente accessibili *online* (art. 1, par. 2), lett. *c-quater*), direttiva 2003/98/CE, introdotta dall'art. 1, par. 1), lett. *a*), punto *iii*), direttiva 2013/37/UE). Com'è noto, l'art. 4, comma 1, lett. *a*), del decreto del 2006 fa salva la disciplina in materia di protezione dei dati personali di cui al Codice (clausola di salvaguardia) e tale disposizione è stata confermata. Oltre a ciò, l'art. 1 del nuovo decreto reca modifiche al decreto del 2006 in linea con le innovazioni della direttiva e in termini compatibili con i princìpi e le garanzie dettate in materia di protezione dei dati personali, anche sulla base delle indicazioni rese dal Garante in occasione del parere reso sullo schema di decreto (parere 23 aprile 2015, n. 239, doc. web n. 3959470). In particolare sono ora compresi, fra i documenti cui si applica il decreto, quelli i cui diritti di proprietà intellettuale sono detenuti dalle biblioteche, comprese le biblioteche universitarie, dai musei e dagli archivi; a seguito delle indicazioni rese dal Garante la disposizione normativa prevede che il riutilizzo di tali documenti avvenga in conformità alle disposizioni del Codice riguardanti il trattamento di dati per scopi storici e alle disposizioni del d.lgs. 22 gennaio 2004, n. 42 (codice dei beni culturali e del paesaggio) concernenti la consultabilità dei documenti degli archivi e la tutela della riservatezza; rispondendo integralmente alle indicazioni rese dal Garante e fatta salva, fra le altre, la disciplina in materia di prote-

zione dei dati personali, sono esclusi dall'accesso i documenti, o le parti di documenti, che contengono dati personali che non sono conoscibili da chiunque o la cui conoscibilità è subordinata al rispetto di determinati limiti o modalità, in base alle leggi, ai regolamenti o alla normativa dell'Unione europea, nonché quelli che contengono dati personali il cui riuso è incompatibile con gli scopi originari del trattamento ai sensi dell'art. 11, comma 1, lett. *b*), del Codice e delle altre disposizioni rilevanti in materia (artt. 1, comma 3, e 3, comma 1, lett. h-*quater*), d.lgs. n. 36/2006).

3 I rapporti con il Parlamento e le altre Istituzioni

3.1. *Le segnalazioni al Parlamento e al Governo*

Anche nel 2015 il Garante – nell'espletamento del compito espressamente attribuito dalla legge – ha segnalato al Parlamento e al Governo l'opportunità di interventi normativi volti ad assicurare le dovute tutele ai diritti degli interessati e in particolare al diritto alla protezione dei dati personali, anche in relazione all'evoluzione registrata in determinati settori (art. 154, comma 1, lett. *f*), del Codice).

Gli interventi del Garante hanno riguardato le seguenti tematiche:

a) Razionalizzazione del quadro sanzionatorio previsto dal Codice.

Una segnalazione indirizzata al Ministro della giustizia ed ai Presidenti delle Commissioni giustizia e bilancio dei due rami del Parlamento (nota 26 novembre 2015, doc. web n. 4575782) in relazione alla riforma presentata dal Governo della disciplina sanzionatoria e di depenalizzazione (AG 245 e 246). L'Autorità ha sostanzialmente reiterato la richiesta – già inoltrata nel 2014 con segnalazione indirizzata anche al Presidente del Consiglio dei ministri e al Ministro per la semplificazione e la pubblica amministrazione (cfr. Relazione 2014) – di alcuni mirati interventi di modifica del Codice volti alla semplificazione degli adempimenti cui sono tenuti i titolari del trattamento e del quadro sanzionatorio, con ridefinizione dei confini tra le fattispecie penali e amministrative e riduzione dei costi per i soggetti destinatari di sanzioni mediante il ricorso a modalità di estinzione agevolata dei procedimenti, nonché ad un aggiornamento delle misure minime di sicurezza (art. 36). In relazione alla precedente proposta di riforma del sistema – che, si badi, contribuirebbe ad uno snellimento degli oneri a carico delle imprese, senza tuttavia abbassare lo *standard* delle garanzie per i cittadini e nel rispetto dei vincoli dell'Unione europea, il Ministro della giustizia assicurò che il contributo del Garante sarebbe stato tenuto nella dovuta considerazione, preferibilmente con il coinvolgimento del Parlamento ed eventualmente mediante il ricorso alla delega legislativa. Dispiace rilevare che, allo stato, né il Governo, né il Parlamento abbiano assunto iniziative normative nella direzione indicata dal Garante.

b) Trattamento dei dati concernenti la cd. scatola nera in dotazione agli autoveicoli.

Una segnalazione, indirizzata alla Commissione attività produttive, commercio e turismo della Camera dei deputati sulle disposizioni del disegno di legge in materia di concorrenza (allo stato ancora all'esame del Parlamento), concernente le possibili implicazioni in materia di protezione dei dati personali dell'installazione sui veicoli della cd. scatola nera (nota 1° luglio 2015, doc. web n. 4575966). Nell'occasione il Garante ha preso atto favorevolmente di come il nuovo dettato normativo avesse accolto le indicazioni già precedentemente suggerite dall'Autorità (in una nota del 2014 indirizzata alla medesima Commissione; cfr. Relazione 2014) circa la standardizzazione dei formati dei dati generati dalle *black box* e di altri parametri del loro funzionamento, con disposizioni più garantiste per gli interessati come, ad es., il divieto di utilizzare i dispositivi per raccogliere dati ulteriori rispetto

a quelli necessari al perseguimento della finalità prevista e di rilevare la posizione del veicolo in maniera continuativa o sproporzionata; l'Autorità ha segnalato, però, l'esigenza di definire ulteriori presìdi per il diritto alla protezione dei dati degli utenti, individuando le tipologie di dati personali trattati rispetto alla finalità perseguita e disciplinando le modalità e i tempi di conservazione delle informazioni e i profili della sicurezza.

c) Legislazione regionale in materia di trasparenza.

Una segnalazione indirizzata al Sottosegretario alla Presidenza del Consiglio con delega agli affari regionali (nota 20 luglio 2015, doc. web n. 4758997), nonché al presidente della Conferenza delle regioni e delle province autonome, riguardante la generale problematica degli interventi legislativi regionali in materia di diffusione di informazioni per finalità di trasparenza amministrativa "in deroga" alla normativa statale (d.lgs. n. 33/2013). Prendendo spunto da alcune segnalazioni ricevute e dal monitoraggio svolto dall'Autorità sulla normativa regionale, il Garante ha richiamato l'attenzione del Governo e della Conferenza delle regioni sulle implicazioni che possono derivare da iniziative legislative delle regioni, qualora introducano nuovi e ulteriori obblighi di diffusione di dati personali rispetto a quelli già previsti dalla normativa statale, anche in relazione ai pertinenti parametri costituzionali e per scongiurare disparità di trattamento fra cittadini.

3.2. *Le audizioni del Garante in Parlamento*

Nel 2015 il Garante ha partecipato ad alcune audizioni presso Commissioni parlamentari o altri organismi anche bicamerali su temi di interesse all'esame del Parlamento, nell'ambito di indagini conoscitive o nel corso dei lavori per l'approvazione di progetti di legge, segnalandone i riflessi in materia di protezione dei dati personali. In questo quadro si collocano, in particolare:

a) un'audizione tenutasi il 26 novembre 2015 presso le Commissioni riunite giustizia e affari sociali della Camera dei deputati nel corso dei lavori parlamentari per l'approvazione di una proposta di legge in materia di prevenzione e contrasto del fenomeno del *cyberbullismo* (doc. web n. 4452702);

b) due audizioni – tenuresi il 9 e il 14 luglio 2015 rispettivamente presso le Commissioni lavoro della Camera e del Senato – sugli schemi di decreti legislativi attuativi della legge-delega 10 dicembre 2014, n. 183 in materia di riforma del lavoro (cd. *Jobs Act*), all'esame delle Commissioni per il prescritto parere (doc. web n. 4119045) (per un primo commento dei decreti legislativi poi adottati dal Governo di maggiore interesse per l'Autorità – nn. 150 e 151 – anche in relazione a quanto osservato dal Garante nell'audizione, cfr. *supra*: par. 2.1.2);

c) un'audizione del 25 marzo 2015 presso la Commissione parlamentare di vigilanza sull'Anagrafe tributaria nell'ambito dell'indagine conoscitiva sull'Anagrafe tributaria nella prospettiva di una razionalizzazione delle banche dati pubbliche in materia economica e finanziaria, che ha riguardato il delicato tema delle grandi banche dati pubbliche e i profili di applicazione della normativa in materia di protezione dei dati personali anche a fini di contrasto dell'evasione fiscale (doc. web n. 3809716);

d) un'audizione tenutasi il 4 marzo 2015 presso le Commissioni riunite giustizia e difesa della Camera sul disegno di legge di conversione del d.l. n.

7/2015 recante Disposizioni in tema di lotta al terrorismo (doc. web n. 3766525) (per un commento delle disposizioni di interesse del provvedimento d'urgenza, anche in relazione a quanto osservato dal Garante nell'audizione, cfr. *supra*: par. 2.1.1);

e) un'audizione tenutasi il 3 marzo 2015 presso il Comitato parlamentare di controllo sull'attuazione dell'accordo di Schengen e di vigilanza sull'attività di Europol in materia di immigrazione, in tema di problematiche connesse alla protezione dei dati personali rispetto al fenomeno dell'immigrazione (doc. web n. 3766836);

f) un'audizione tenutasi il 12 gennaio 2015 presso la Commissione sui diritti e i doveri relativi ad internet, istituita presso la Camera dei deputati, sulla Dichiarazione dei diritti in Internet (doc. web n. 3652679).

3.3. *L'Autorità e le attività di sindacato ispettivo e di indirizzo e controllo del Parlamento*

L'Autorità ha fornito la consueta collaborazione al Governo in riferimento ad atti di sindacato ispettivo e ad attività di indirizzo e di controllo del Parlamento riguardanti aspetti di specifico interesse in materia di protezione dei dati personali (cfr. sez. IV, tab. 11). In particolare, sono stati forniti elementi di valutazione ai fini della risposta, da parte del Governo, su:

a) un'interrogazione in materia di repressione del fenomeno della violenza via web, con particolare riferimento al fenomeno del cd. *cyberbullismo* (n. 4-01695 della sen. Alberti Casellati – nota 22 dicembre 2015);

b) una mozione in materia di *governance* della rete e dichiarazione dei diritti e doveri in internet (n. 1-01031 dell'on. Quintarelli – nota 30 ottobre 2015);

c) una mozione in materia di misure a tutela dei lavoratori di *call center* delocalizzati (n. 1-00933 dell'on. Petraroli – nota 8 ottobre 2015);

d) un'analoga interrogazione a risposta scritta in materia di *call center* e applicazione dell'art. 24-*bis*, d.l. n. 134/2012 (n. 4-08238 dell'on. Catanoso Genoese – nota 8 ottobre 2015);

e) un'interrogazione a risposta scritta in materia di tutela del diritto alla salute e alla riservatezza di una donna transessuale (n. 4-04392 dell'on. Zan – nota 25 settembre 2015);

f) una mozione circa gli obblighi di comunicazione cui sono tenuti gli istituti di credito nei rapporti con la clientela previsti dal t.u. bancario e la Centrale dei rischi (n. 1-00723 dell'on. Petraroli ed altri – nota 26 aprile 2015);

g) un'interpellanza urgente in merito alla delega prevista dall'art.1, comma 7, lett. *f*), l. n. 183/2014 in materia di controlli a distanza sugli impianti e sugli strumenti di lavoro (n. 2-00927 dell'on. Ciprini ed altri – nota 16 aprile 2015).

3.4. *L'attività consultiva del Garante sugli atti del Governo*

3.4.1. I pareri sugli atti regolamentari e amministrativi del Governo

Nel quadro dell'attività consultiva obbligatoria concernente norme regolamentari ed atti amministrativi suscettibili di incidere sulla protezione dei dati personali (art. 154, comma 4, del Codice), il Garante ha espresso il parere (obbligatorio) di

competenza sugli schemi di numerosi provvedimenti (cfr. sez. IV, tab. 3), di seguito riportati:

1) decreto del Ministro dell'economia e delle finanze di attuazione della l. 18 giugno 2015, n. 95, e della direttiva 2014/107/UE del Consiglio del 9 dicembre 2014, recante modifica della direttiva 2011/16/UE in materia di scambio automatico obbligatorio di informazioni nel settore fiscale (parere 17 dicembre 2015, n. 661, doc. web n. 4634033, cfr. par. 4.6);

2) convenzione fra l'Agenzia per l'Italia Digitale (AgID) ed i gestori di identità digitale, da adottare ai sensi dell'art. 10, comma 2, d.P.C.M. 24 ottobre 2014 recante la "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (Spid)" e aggiornamento al regolamento AgID recante le modalità attuative per la realizzazione dello Spid (parere 17 dicembre 2015, n. 660, doc. web n. 4538528);

3) decreto del Ministro dell'interno recante le modalità tecniche di emissione della Carta d'identità elettronica (Cie) (parere 17 dicembre 2015, n. 656, doc. web n. 4634495, cfr. par. 4.4);

4) decreto del Ministro della salute concernente l'istituzione del sistema informativo per il Monitoraggio della rete di assistenza (Mra) (parere 17 dicembre 2015, n. 657, doc. web n. 4630606);

5) decreto direttoriale congiunto del Direttore centrale per i servizi demografici del Ministero dell'interno e del Direttore centrale delle statistiche socio-demografiche e ambientali dell'Istituto nazionale di statistica, che definisce gli *standard* e gli indicatori finalizzati a monitorare la qualità dei dati registrati nell'Anpr nella fase di subentro delle anagrafi comunali, in attuazione dell'art. 1, comma 3, d.P.C.M. 10 novembre 2014, n. 194 (parere 17 dicembre 2015, n. 655, doc. web n. 4575714, cfr. par. 4.2);

6) provvedimento del Responsabile dei sistemi informativi automatizzati del Ministero della giustizia, ai sensi degli artt. 3, comma 5, e 4, comma 5, d.m. 19 settembre 2013, n. 160, in materia di albo degli amministratori giudiziari (parere 2 dicembre 2015, n. 630, doc. web n. 4633969); si tratta di un secondo parere reso su un testo modificato dal Dicastero in base al precedente parere del 30 luglio 2015 (v. n. 16);

7) decreto del Ministro della giustizia recante la disciplina delle modalità di iscrizione in via telematica degli arti di ultima volontà nel registro generale dei testamenti su richiesta del notaio o del capo dell'archivio notarile, ai sensi dell'arr. 5-*bis* l. n. 307/1981 (parere 25 novembre 2015, n. 618, doc. web n. 4538494);

8) d.P.C.M. di modifica al d.P.C.M. 24 maggio 2010 recante le regole tecniche delle Tessere di riconoscimento (mod. AT) di cui al d.P.R. n. 851 del 1967 rilasciate con modalità elettronica (parere 18 novembre 2015, n. 603, doc. web n. 4582514);

9) d.P.C.M. concernente regolamento recante le regole tecnico-operative per l'attuazione del processo amministrativo telematico (parere 29 ottobre 2015, n. 565, doc. web n. 4582442);

10) provvedimento del Responsabile per i sistemi informativi automatizzati del Ministero della giustizia recante modifiche al provvedimento 16 aprile 2014, in materia di specifiche tecniche del processo telematico (parere 22 ottobre 2015, n. 549, doc. web n. 4582365);

11) d.P.C.M. in materia di censimento della popolazione e delle abitazioni e di Archivio nazionale dei numeri civici e delle strade urbane (Anncsu) (parere 15 ottobre 2015, n. 536, doc. web n. 4481301, cfr. parr. 4.2 e 7.2);

12) regolamento del Ministro dell'istruzione, dell'università e della ricerca per l'integrazione dell'Anagrafe nazionale degli studenti con i dati sulla disabilità degli

alunni (parere 15 ottobre 2015, n. 535, doc. web n. 4448995, cfr. par. 4.5);

13) decreto del Ministro dell'istruzione, dell'università e della ricerca per l'integrazione dell'Anagrafe nazionale degli studenti con i dati relativi agli iscritti alla scuola dell'infanzia (parere 8 ottobre 2015, n. 522, doc. web n. 4448919, cfr. par. 4.5);

14) decreto del Ministro della difesa recante le modalità per l'adozione del sistema del doppio certificato per il personale militare di cui all'art. 748, comma 2, d.P.R. n. 90 del 15 marzo 2010 (parere 8 ottobre 2015, n. 521, doc. web n. 4487512);

15) decreto del Ministro degli affari esteri e della cooperazione internazionale e decreto del Direttore generale per gli italiani all'estero e le politiche migratorie in tema di dati biometrici nei documenti di viaggio elettronici (parere 30 luglio 2015, n. 453, doc. web n. 4243396);

16) provvedimento del Responsabile dei sistemi informativi automatizzati del Ministero della giustizia emesso ai sensi degli artt. 3, comma 5, e 4, comma 5, d.m. n. 160, 19 marzo 2013, in materia di Albo degli amministratori giudiziari (parere 30 luglio 2015, n. 452, doc. web n. 4252526);

17) decreto del Ministero delle finanze relativo alle modalità di trasmissione telematica delle spese sanitarie al Sistema tessera sanitaria da rendere disponibili all'Agenzia delle entrate ai fini dell'elaborazione della dichiarazione dei redditi precompilata (parere 30 luglio 2015, n. 450, doc. web n. 4160058, cfr. par. 4.6);

18) provvedimento del Direttore dell'Agenzia delle entrate concernente le modalità tecniche di utilizzo dei dati delle spese sanitarie ai fini della elaborazione della dichiarazione dei redditi precompilata (parere 30 luglio 2015, n. 451, doc. web n. 4160102, cfr. par. 4.6);

19) provvedimento del Direttore dell'Agenzia delle entrate recante disposizioni di attuazione del decreto del Ministero delle finanze, attuativo della l. n. 95/2015 (ratifica dell'Accordo FATCA), concernente le modalità e i termini di trasmissione all'Agenzia delle entrate dei dati oggetto di comunicazione da parte degli intermediari finanziari (parere 23 luglio 2015, n. 438, doc. web n. 4252461, cfr. par. 4.6);

20) d.P.C.M. attuativo delle disposizioni di cui all'art. 12, comma 11, d.l. 18 ottobre 2012, n.179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221, in materia di "sistemi di sorveglianza e registri" (parere 23 luglio 2015, n. 435, doc. web n. 4252386, cfr. par. 5.2.1);

21) d.P.R. di recepimento della direttiva 2012/39/UE concernente prescrizioni tecniche relative agli esami effettuati su tessuti e cellule umane (parere 8 luglio 2015, n. 412, doc. web n. 4243488);

22) decreto del Ministro dell'economia e delle finanze attuativo della l. n. 95/2015, recante la ratifica dell'Accordo Italia-USA finalizzato a migliorare la *compliance* fiscale internazionale e ad applicare la normativa FATCA (*Foreign Account Tax Compliance Act*) (parere 8 luglio 2015, n. 411, doc. web n. 4160287, cfr. par. 4.6);

23) decreto del Presidente della Corte dei conti *ex* art. 20-*bis*, d.l. 18 ottobre 2012, n. 179, convertito dalla l. 17 dicembre 2012, n. 221, concernente istruzioni tecnico-operative per l'utilizzo della posta elettronica certificata nei giudizi innanzi alla Corte dei conti (parere 8 luglio 2015, n. 410, doc. web n. 4243453);

24) decreti del Ministro dell'istruzione, dell'università e della ricerca riguardanti le modalità e i contenuti delle prove di ammissione ai corsi di laurea ad accesso programmato per l'anno accademico 2015-2016 (in italiano e in inglese) (parere 2 luglio 2015, n. 392, doc. web n. 4241082);

25) decreto del Ministro della salute recante disposizioni relative ai requisiti di qualità e sicurezza del sangue e degli emocomponenti (*ex* artt. 3 e 21, l. 21 ottobre

2005, n. 219) (parere 25 giugno 2015, n. 379, doc. web n. 4172235, cfr. par. 5.2.1);

26) decreto del Ministro delle politiche agricole, alimentari e forestali recante l'istituzione del Registro unico dei controlli ispettivi sulle imprese agricole (Ruci), da adottare ai sensi dell'art. 1, commi 1 e 2, d.l. 24 giugno 2014, n. 91, convertito, con modificazioni, dalla l. 11 agosto 2014, n. 116 (parere 25 giugno 2015, n. 378, doc. web n. 4169267);

27) decreto interministeriale del Ministro del lavoro e delle politiche sociali e del Ministro della salute concernente la definizione delle modalità per la predisposizione e l'invio telematico all'Inps del certificato medico di gravidanza, del certificato di interruzione della gravidanza e del certificato di parto ai sensi dell'art. 21, d.lgs. 26 marzo 2001, n. 151, come modificato dall'art. 34, d.l. 21 giugno 2013, n. 69, convertito con modificazioni dalla l. 9 agosto 2013, n. 98 (parere 4 gingno 2015, n. 334, doc. web n. 4130998, cfr. par. 5.2);

28) Linee di guida del Ministero della salute riguardanti la possibilità che la carta d'identità possa contenere il consenso o il diniego alla donazione di organi o tessuti in caso di morte (parere 4 giugno 2015, doc n. 333, web n. 4070710, cfr. par. 4.4);

29) regolamenti della Presidenza del Consiglio dei ministri – AgID recanti le modalità attuative per la realizzazione del Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (Spid) e le relarive regole tecniche (parere 4 giugno 2015, n. 332, doc. web n. 4257475);

30) decreto del Ministro della salute recante attuazione della direrriva 2010/53/UE sulle norme di qualità e sicurezza degli organi umani destinati ai trapianti, ai sensi dell'art. 1, comma 340, l. 24 dicembre 2012, n. 228, nonché in attuazione della direttiva di esecuzione 2012/25/UE in materia di procedure informative per lo scambio tra gli Stati membri di organi destinati ai trapianti, nonché in attuazione dell'art. 7, l. n. 91 del 1999 (parere 28 maggio 2015, n. 315, doc. web n. 4168076, cfr. par. 5.2.1);

31) decreto del Direttore generale delle finanze del Ministero dell'economia e delle finanze concernente le regole tecnico-operative per l'utilizzo di strumenti informatici e telematici nel processo ttibutario (poi d.m. 4 agosto 2015; parere 28 maggio 2015, n. 314, doc. web n. 4070757);

32) decreto del Ministero dell'istruzione, dell'università e della ticerca recante la regolamentazione per la realizzazione e consegna della Carta dello Studente denominata "IoStudio" (parere 28 maggio 2015, n. 313 doc. web n. 4070802, cfr. par. 4.5);

33) decreto del Ministro degli affari esteri e della cooperazione internazionale sulle caratteristiche di sicurezza e sugli elementi biometrici dei documenti di viaggio per apolidi, rifugiati e stranieri (poi d.m. 7 maggio 2015; parere 30 aprile 2015, n. 257, doc. web n. 4015181);

34) regolamento dell'AgID in attuazione dell'art. 4, comma 4, d.P.C.M. 24 ottobre 2014, recante le procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello Spid, il rilascio dell'identità digirale (parere 23 aprile 2015, n. 237, doc. web n. 3953079);

35) regolamento dell'AgID in attuazione dell'art. 4, comma 3, d.P.C.M. 24 ottobre 2014, recante le modalirà per l'accreditamento e la vigilanza sui gestori dell'identità digitale (parere 23 aprile 2015, n. 238, doc. web n. 3953181);

36) decreto del Ministro della salute in materia di *screening* neonatale esteso (sne) (parere 2 aprile 2015, n. 196, doc. web n. 3943315, cfr. par. 5.2.1);

37) decreto del Ministro dell'interno di concerto con il Ministro delle infrastrutture e dei trasporti *ex* art. 5, comma 2, d.lgs. n. 37/2014 recante il recepimento della

direttiva europea 2011/82/UE del Parlamento europeo e del Consiglio, intesa ad agevolare lo scambio transfrontaliero di informazioni sulle infrazioni in materia di sicurezza stradale, concernente l'accesso del Ministero delle infrastrutture e dei trasporti ad informazioni sui veicoli rubati (poi d.m. 4 agosto 2015; parere 26 marzo 2015, n. 180, doc. web n. 3871227);

38) decreto del Ministro della salute recante modifiche e integrazioni al d.m. 27 ottobre 2000, n. 380, concernente le schede di dimissione ospedaliera (Sdo) (parere 26 marzo 2015, n. 178, doc. web n. 3878687, cfr. par. 5.2.1);

39) decreto del Direttore centrale dell'immigrazione e della polizia delle frontiere del Ministero dell'interno recante prescrizioni tecniche in materia di "modalità di acquisizione e di verifica degli elementi biometrici primari e secondari" del permesso di soggiorno elettronico (art. 10, comma 1, lett. *c*), d.m. 23 luglio 2013) (parere 19 marzo 2015, n. 163, doc. web n. 3871124);

40) decreto del Ministro della salute recante procedure per l'interconnessione dei sistemi informativi su base individuale del Ssn, anche quando gestiti da diverse amministrazioni dello Stato (art. 15, comma 25-*bis*, del d.l. 6 luglio 2012, n. 95, convertito, con modificazioni, dalla l. n. 135/2012) (parere 19 marzo 2015, n. 162, doc. web n. 3869889, cfr. par. 5.2.1);

41) decreto del Direttore centrale dell'immigrazione e della polizia delle frontiere del Ministero dell'interno recante prescrizioni tecniche concernenti l'"infrastruttura di sicurezza pse" per la produzione e il rilascio del permesso di soggiorno elettronico (art. 10, comma 1, lett. *b*), d.m. 23 luglio 2013) (parere 12 marzo 2015, n. 141, doc. web n. 3858699);

42) decreto del Direttore centrale dell'immigrazione e della polizia delle frontiere del Ministero dell'interno e della cooperazione internazionale recante prescrizioni tecniche relative a "procedure e processi di produzione e di servizio per il procedimento di emissione e controllo del permesso di soggiorno" (art. 10, comma 1, lett. *a*), d.m. 23 luglio 2013) (parere 5 marzo 2015, n. 119, doc. web n. 3816200);

43) decreto del Ministro dell'economia e delle finanze recante disposizioni relative al controllo dell'autenticità e dell'idoneità alla circolazione delle monete metalliche in euro (poi d.m.. 21 aprile 2015; parere 29 gennaio 2015, n. 48, doc. web n. 3750475);

44) d.P.R. recante adeguamento del regolamento anagrafico della popolazione residente approvato con d.P.R. 30 maggio 1989, n. 223, alla disciplina istitutiva dell'anagrafe nazionale della popolazione residente (poi d.P.R. 17 luglio 2015, n. 126; parere 22 gennaio 2015, n. 31, doc. web n. 3738655, cfr. par. 4.4).

Si sottolinea che nel 2015 si è registrato un incremento esponenziale dell'attività consultiva del Garante, con un numero di pareri resi dall'Autorità doppio rispetto all'anno precedente.

Tali importanti risultanze si giustificano alla luce della produzione normativa particolarmente intensa di taluni Dicasteri e della generale accresciuta sensibilità delle Amministrazioni in ordine alla necessità di approfondire gli aspetti di protezione dei dati personali e all'utilità della consultazione del Garante, anche al di là dell'obbligo di legge.

3.4.2. I pareri su norme di rango primario

L'Autorità è stata coinvolta dalla Presidenza del Consiglio dei ministri nella fase preparatoria di alcuni atti normativi aventi rango primario.

In un caso è stato richiesto il parere formale del Garante sullo schema di decreto legislativo di attuazione della direttiva 2013/37/UE del 26 giugno 2013 (che modifica la direttiva 2003/98/CE) concernente il riutilizzo dell'informazione del settore

pubblico (poi d.lgs. 18 maggio 2015, n. 102; parere 23 aprile 2015, n. 239, doc. web n. 3959470).

È stata altresì richiesta la collaborazione dell'Aurorità durante la fase di studio e preparazione dello schema di decreto legislarivo recante l'attuazione della decisione quadro 2006/960/GAI del Consiglio relativa alla semplificazione dello scambio di informazioni e *intelligence* tra le Autorità degli Stati UE ai fini dello svolgimento di indagini penali o di operazioni di *intelligence* criminale (poi d.lgs. 23 aprile 2015, n. 54).

Al riguardo occorre considerare che l'art. 154, comma 4, del Codice fa riferimento alla normariva avente rango secondario, anche se la correlata disposizione della direttiva europea non reca una distinzione al riguardo (art. 28, par. 2). Le richieste di parere su atti primari si inquadrano in un contesto di collaborazione con le amministrazioni interessate che l'Autorità, come più volte segnalato alla Presidenza del Consiglio, auspica possa ulteriormenre svilupparsi, nella consapevolezza che sia di grande utilirà il coinvolgimento del Garante nella fase preparatoria di iniziative legislarive, olrre che regolamenrari, del Governo al fine di valurarne previamente l'impatto sulla protezione dei dati personali e sui diritti delle persone.

3.5. *L'esame delle leggi regionali*

È proseguita l'attività di esame del Garante delle leggi regionali approvate e sottoposte al vaglio di costituzionalità del Governo ai sensi dell'art. 127 della Costituzione, al fine di fornire alla Presidenza del Consiglio dei ministri eventuali elementi di valutazione circa la compatibilità di esse con le disposizioni in materia di protezione dei dati personali e con il dettaro costituzionale (art. 117, comma 2, lett. *l*), Cost.).

L'Autorità, nel corso dell'anno, ha esaminato 14 leggi regionali e, in linea generale, ha riscontrato un sostanziale corretto svolgimento della potestà legislativa regionale in relazione agli aspetti di protezione dei dari personali, salvo quanto di seguito esposto.

In un primo caso il Garante ha rirenuro necessario segnalare alla Presidenza del Consiglio dei ministri profili di possibile illegittimità riferiti alla legge della Regione Sicilia n. 22/2015 recante l'istituzione di biobanche in Sicilia (cfr. par. 6).

La legge riguardava l'istituzione in Sicilia di una biobanca di ricerca (Bbr), per la raccolta, la lavorazione, la conservazione e la distribuzione ad enti e gruppi di ricerca regionali, nazionali ed internazionali di materiale biologico umano, raccolto in molteplici ambiti clinici, specificatamente prelevato da pazienti, nonché di *surplus* di materiale derivato da interventi diagnostici o terapeutici, ovvero donato per trapianto e non idoneo allo scopo, senza però alcuna indicazione in merito alla destinazione e all'uso dei dati personali (art. 1). La disposizione, in particolare, non indicava le specifiche finalità in grado di giustificare l'acquisizione, la conservazione e, tanto più, la distribuzione generalizzata dei predetti dati e campioni "ad enti e gruppi di ricerca regionali, nazionali e internazionali".

L'Autorità ha al riguardo rilevato che, ove non integrata dalla Regione con l'indicazione espressa delle specifiche finalità perseguibili in conformità alla pertinente disciplina nazionale in materia di dati genetici (art. 90 del Codice e autorizzazione del Garante n. 8/2014), la legge si sarebbe posta in contrasto con i princìpi e le regole sulla protezione dei dati personali e genetici codificati a livello nazionale e, per l'effetto, con il dettato costituzionale (art. 117, comma 2, lett. *l*), Cost.), non potendo la Regione disciplinare la prorezione dei dati genetici in maniera difforme

dal Codice e invadere così una competenza riservata esclusivamente allo Stato (nota 19 novembre 2015).

Con successiva nota del 25 novembre 2015 il Presidente della Giunta della Regione siciliana ha comunicaro alla Presidenza del Consiglio l'impegno del governo regionale a presentare un nuovo disegno di legge appositamente emendato secondo le osservazioni del Garante.

Il Garante è altresì intervenuto in merito alla legittimità costituzionale della legge della Regione Friuli-Venezia Giulia n. 4 del 13 marzo 2015, che intendeva istituire il registro regionale per le dichiatazioni anticipate di trattamento sanitario (Dat) e recava disposizioni per favorire la raccolta delle volontà di donazione degli organi e dei tessuti.

Nella nota indirizzata alla Presidenza del Consiglio (7 maggio 2015), l'Autorità – richiamata l'attenzione sugli artt. 2, commi 3 e 4, e 6 della legge – ha rilevato che per operare correttamente il trattamento di dati personali, comuni e sensibili, implicato dalla Dat occorre che il trattamento inerisca allo svolgimento delle funzioni istituzionali delle aziende per l'assistenza sanitaria (art. 18, comma 2, del Codice) e che una norma di rango statale individui le finalità di rilevante interesse pubblico alla base dello stesso, secondo quanto previsto dall'art. 20 del Codice. Né è apparso possibile effettuare l'individuazione della rilevante finalità di interesse pubblico con un regolamento regionale (a cui rinviava l'art. 9 della l.r.).

Secondo quanto stabilito dalla Corte costituzionale con la sentenza n. 271/2005, infatti, il predetto art. 20 del Codice, al comma 2, ammette "solo l'integrazione delle prescrizioni legislative statali che siano incomplete in relazione al trattamento di dati sensibili da parte di pubbliche amministrazioni (poiché non determinano 'i tipi di dati sensibili e di operazioni eseguibili') ..... operata tramite appositi regolamenti 'a cura dei soggetti che ne effettuano il trattamento', seppure 'in conformità al parere espresso dal Garante ai sensi dell'art. 154, comma 1, lettera *g*), anche su schemi tipo'. In questi ambiti possono quindi essere adottati anche leggi o regolamenti regionali, ma solo in quanto e nella misura in cui ciò sia appunto previsto dalla legislazione statale".

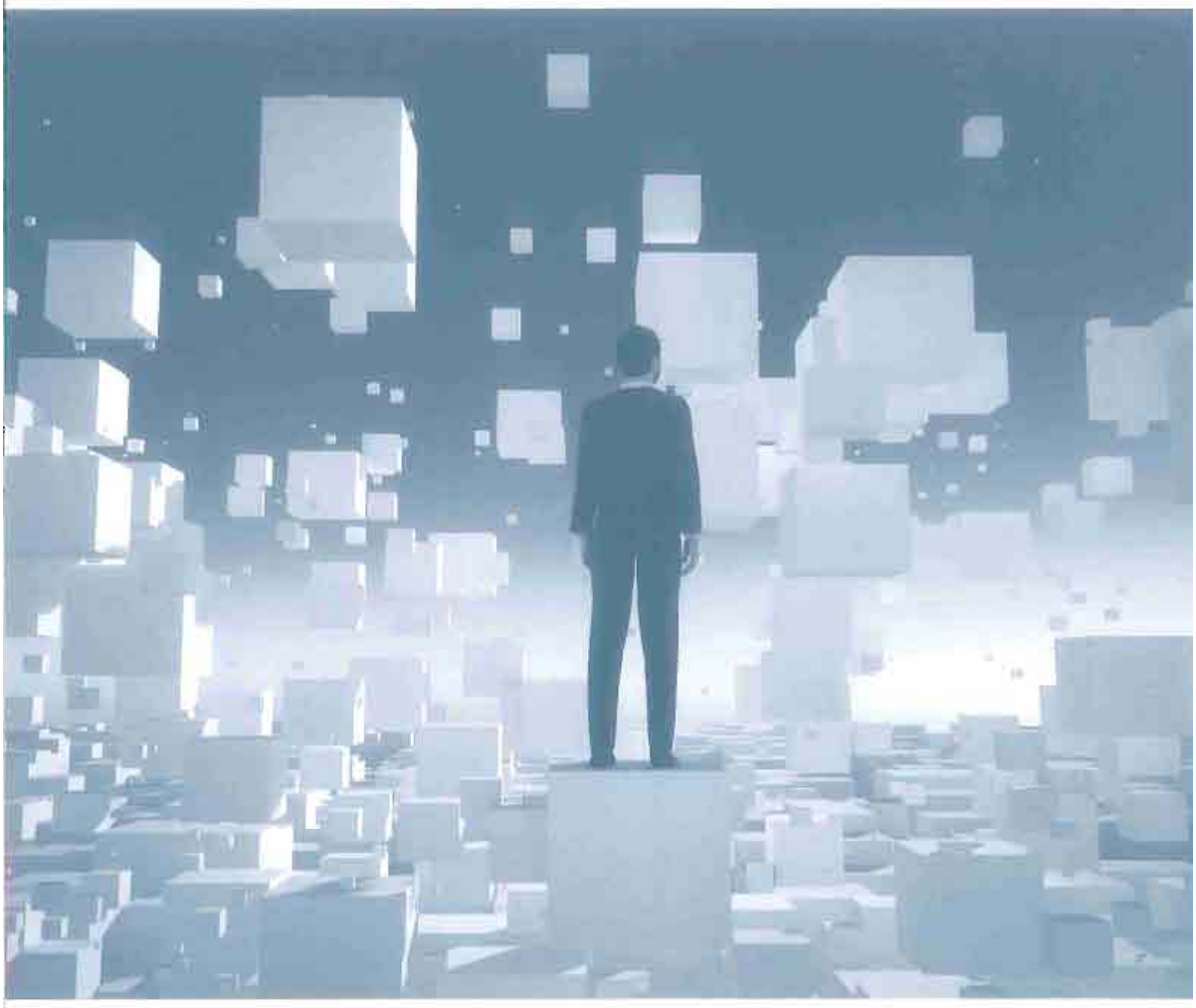
La legge regionale è stata impugnata dal Governo con deliberazione del Consiglio dei ministri del 18 maggio 2015 anche sulla scorta degli elementi forniti dall'Autorità.

Successivamente la Presidenza del Consiglio ha chiesto nuovamente elementi al Garante in merito ad una legge con la quale la Regione modificava la legge impugnata (l. n. 22/2015). A fronte del nuovo testo trasmesso, l'Autorità, constatata la perdurante mancanza nell'ordinamento di una normativa statale in materia di Dat, ha preso atto che le modifiche apportate non attenevano agli aspetti segnalati nella prima occasione e ha confermato il contenuto della nota del maggio 2015 relativa alla l. n. 4/2015 (nota 31 luglio 2015).

Infine, in relazione ad una legge della Regione Lazio in materia di trasparenza (l. n. 12/2015), l'Autorità ha inoltrato alla Presidenza del Consiglio copia delle proprie note con le quali aveva segnalato al Governo e alla Conferenza delle regioni la problematica delle implicazioni che possono derivare da iniziative legislative regionali che introducano, eventualmente, nuovi ed ulteriori obblighi di diffusione di dati personali rispetto a quelli già previsti dalla normativa statale (v. par. 3.1).

PAGINA BIANCA

L'attività svolta dal Garante



PAGINA BIANCA

II - L'attività svolta dal Garante

4 Il Garante e le pubbliche amministrazioni

4.1. *I trattamenti di dati sensibili e giudiziari presso le amministrazioni pubbliche*

La Banca d'Italia ha chiesto il parere del Garante in ordine a uno schema di regolamento sul trattamento dei dati sensibili e giudiziari che abroga e sostituisce quello adottato dall'Istituto il 22 marzo 2011. L'aggiornamento è motivato dall'esigenza di introdurre un nuovo sistema per lo scambio di informazioni tra i prestatori dei servizi di pagamento comprensivo anche di dati identificativi dell'ordinante e del beneficiario, nonché della causale del pagamento.

Il parere favorevole reso dall'Autorità ha riguardato una versione aggiornata dello schema di regolamento che ha tenuto in considerazione gli approfondimenti e le indicazioni rese per le vie brevi dall'Ufficio, in particolare, in relazione all'integrazione delle fonti normative legittimanti il trattamento dei predetti dati, la selezione delle finalità di rilevante interesse pubblico perseguite e il perfezionamento della descrizione del trattamento effettuato dall'Istituto per la gestione del nuovo sistema Cabi per lo scambio di informazioni di pagamento tra i prestatori di tali servizi (provv. 10 settembre 2015, n. 469, non pubblicato ai sensi dell'art. 24 del reg. Garante 1° agosto 2013).

La Banca d'Italia ha chiesto, altresì, di essere autorizzata a trattare i dati giudiziari dei dipendenti delle ditte appaltatrici di servizi e/o lavori, manutentori, consulenti ed altri soggetti autorizzati a titolo continuativo ad accedere agli ambienti sensibili sotto il profilo della sicurezza.

A seguito degli approfondimenti condotti, è stato circoscritto il numero di soggetti da sottoporre ai controlli preventivi, le aree da considerare sensibili sotto il profilo della sicurezza e i reati suscettibili di precludere l'impiego di tali soggetti presso i predetti locali.

È stato altresì stabilito che l'informativa deve specificare le informazioni acquisibili presso il casellario giudiziario e il previsto divieto ad accedere agli ambienti sensibili qualora i controlli evidenzino precedenti critici.

Il Garante, nel rispetto dell'autorizzazione n. 7/2014, ha pertanto autorizzato la Banca d'Italia al trattamento dei dati giudiziari indispensabili alla predetta attività di controllo (provv. 18 giugno 2015, n. 357, doc. web n. 4172355).

4.2. *L'amministrazione digitale*

Spid

Come illustrato nella Relazione 2014 (cfr. p. 34), con d.P.C.M. 24 ottobre 2014, è stato avviato il processo di definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini ed imprese (Spid), nonché dei tempi e delle modalità di adozione del sistema Spid da parte delle pp.aa. e delle imprese.

La realizzazione di un'infrastrutrura sicura e affidabile di verifica dell'identità in rete di cittadini e imprese costituisce un passaggio indispensabile per l'intero percorso di digitalizzazione del Paese.

Nel 2015 AgID ha emanato i relativi regolamenti attuativi coinvolgendo l'Autorità affinché fossero assicurati elevati livelli di sicurezza e solide garanzie di prorezione dati.

L'Autorità si è pronunciata attraverso quattro distinti pareri:

- provv. 23 aprile 2015, n. 237 (doc. web 3953079), sullo schema di regolamento recante le procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello Spid, il rilascio dell'identità digitale;
- provv. 23 aprile 2015, n. 238 (doc. web n. 3953181), sullo schema di regolamento recante le modalità per l'accreditamento e la vigilanza sui gestoti dell'identità digitale;
- provv. 4 giugno 2015, n. 332 (doc. web 4257475), sugli schemi di regolamento recanti rispettivamente, le modalità attuative per la realizzazione dello Spid e le relative regole tecniche;
- provv. 17 dicembre 2015, n. 660 (doc. web 4538528), sullo schema di regolamento recante le modalità attuative per la realizzazione dello Spid e sullo schema di convenzione relativa ai gestori dell'identità digitale.

In tutti i casi, pur risultando i testi conformi alla gran parte delle osservazioni formulate dall'Autorità nell'ambito di un tavolo tecnico appositamente istituito, sono state chieste ulteriori specificazioni a maggior garanzie degli interessati, come ad esempio quella di perfezionare la descrizione dei livelli di sicurezza delle identità digitali anche al fine di garantire una maggiore coerenza con quanto previsto all'art. 8 del regolamento (UE) n. 910/2014 del 23 luglio 2014, in materia di livelli di garanzia dei mezzi di identificazione elettronica. L'Autorità ha poi richiesto che le domande di accreditamento dei gestori di identità digitale fossero corredate da un'approfondita analisi dei rischi che tenesse anche in conto le criticità derivanti dall'uso di identità digitali pregresse in fase di richiesta di una nuova identità Spid.

Inoltre, è stato richiesto di garantire che gli utenti (cioè le persone cui è stata attribuita, a richiesta, un'identità digitale) siano messi in grado di comprendere appieno le potenzialità, e quindi anche i rischi, di tale infrastruttura, in quanto, dal punto di vista della sicurezza, il sistema Spid si potrà dire pienamente funzionante solo una volta che gli utenti avranno acquisito una piena consapevolezza sulle corrette modalità di utilizzo del sistema.

Altre osservazioni di rilievo hanno riguardato il "codice utente Spid", costituito necessariamente, nella proposta AgID, da un indirizzo *e-mail*, in luogo di un più semplice codice parlante. Tale vincolo avrebbe però reso indispensabile la tealizzazione di un servizio di *discovery* centralizzato, necessario ad individuare, a partire dall'indirizzo *e-mail* fornito dall'utente in fase di autenticazione ai servizi *online*, il corrispondente gestore di identità digitale. A parere dell'Autorità, l'introduzione nel sistema di tale componente architetturale fortemente centralizzata, avrebbe costituito un evidente *single point of failure*, pericolosamente esposto ad attacchi quali quelli di *distributed denial of service* con effetti potenzialmente pregiudizievoli sull'intero sistema di accesso ai servizi *online* delle pp.aa. e dei service *provider* privati.

È stata infine rafforzata la collaborazione fra l'Autorità e l'AgID relativa all'attività di vigilanza sull'infrastruttura Spid al fine di assicurare un efficace coordinamento dell'attività di *audit* e controllo svolte da AgID e Garante nei rispettivi

ambiti di competenza, sia AgID che i gestori di identità digitale, laddove riscontrino casi di *data breach* che abbiano riflessi sulla protezione dei dati personali, sono tenuti a informare tempestivamente il Garante che si attiverà sulla base alle proprie competenze istituzionali.

4

Data breach e sicurezza

L'Autorità, al fine di innalzare i livelli di tutela dei dati contenuti nelle banche dati delle amministrazioni pubbliche, ha previsto che tutte le amministrazioni pubbliche debbano comunicare al Garante le violazioni o gli incidenti informatici (accessi abusivi, azione di *malware*) che possano mettere a rischio i dati personali ivi contenuti. I cd. *data breach*, quindi, dovranno essere comunicati al Garante, utilizzando un apposito schema, entro quarantotto ore dalla conoscenza del fatto (provv. 2 luglio 2015, n. 393, doc. web n. 4129029). Il Garante, in attesa della definizione degli "*standard* di comunicazione e le regole tecniche" da parte di AgID previsti dalla nuova formulazione dell'art. 58, comma 2, del Cad, ha dettato le misure di sicurezza in ogni caso necessarie. Ciò in considerazione dalla delicatezza delle informazioni contenute nelle banche dati, dell'ingente mole dei dati ivi trattati e dalla molteplicità dei soggetti autorizzati ad accedervi. L'Autorità ha altresì ribadito le misure tecniche e organizzative da predisporre al fine di prevenire il verificarsi di violazioni o di incidenti informatici, già individuate nel 2013 (provv. 4 luglio 2013, n. 332, doc. web n. 2574977), specificando che la mancata comunicazione al Garante dei cd. *data breach*, nonché la mancata adozione delle misure necessarie individuate nel provvedimento, configurano un illecito amministrativo sanzionato ai sensi dell'art. 162, comma 2-*ter* del Codice (cfr. par. 11.7).

Tra le dettagliate misure individuate dall'Autorità vanno segnalate: la redazione da parte della p.a. erogatrice di un documento, costantemente aggiornato, con l'elenco delle banche dati accessibili e dei fruitori esterni autorizzati; la necessità di stipulare comunque una convenzione (ovvero qualsivoglia atto bilaterale) quale strumento con cui le amministrazioni possono stabilire le garanzie a tutela del trattamento dei dati personali e dell'utilizzo dei sistemi informativi; l'identificazione degli utenti (persone fisiche incaricate) che hanno accesso alla banca dati, anche in caso di accessi attraverso web *service*, i quali devono essere esclusivamente integrati con il sistema informativo del fruitore e non possono essere resi disponibili a terzi per via informatica; gli accessi alle banche dati avvengano soltanto tramite l'uso di postazioni di lavoro connesse alla rete Ip dell'ente autorizzato o dotate di certificazione digitale che identifichi univocamente la postazione di lavoro nei confronti dell'erogatore, anche attraverso procedure di accreditamento che consentano di definire reti di accesso sicure (circuiti privati virtuali); l'adeguato tracciamento delle operazioni compiute e la predisposizione di idonee procedure di *audit* sugli accessi alle banche dati; il divieto per il soggetto pubblico fruitore di estrarre dati in via automatica e massiva e di creare nuove banche dati.

Con provvedimento 17 dicembre 2015 (n. 655, doc. web n. 4575714), il Garante ha espresso il parere sullo schema di decreto direttoriale predisposto congiuntamente dal Ministeto dell'interno e dall'Istituto nazionale di statistica, che individua gli *standard* e gli indicatori finalizzati a monitorare la qualità dei dati registrati nell'Anpr nella fase di subentro delle anagrafi comunali, in attuazione dell'art. 1, comma 3, d.P.C.M. 10 novembre 2014, n. 194 "Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente e ridefinizione del piano per il graduale subentro dell'Anpr alle anagrafi della popolazione residente". Lo schema di decreto ha recepito gli approfondimenti e le indicazioni suggeriti dall'Ufficio in relazione all'esigenza di eliminare l'ulteriore indicatore basato sul raffronto dei dati individuali contenuti nell'anagrafe a fini amministrativi con i dati identificativi comunicati all'Istat dai comuni per finalità

statistiche a seguito della revisione *post*-censuaria, in contrasto con il divieto di utilizzare per finalità amministrative dati raccolti per finalità statistiche (cfr. art. 105 del Codice e provv.ti 15 e 29 ottobre 2015, n. 536, doc. web n. 4481301 e n. 566, doc. web n. 4476104).

4.3. *La trasparenza amministrativa*

In materia di diffusione di dati personali *online* per finalità di trasparenza o di pubblicità dell'azione amministrativa il Garante è stato chiamato a pronunciarsi su numerose questioni di cui si riportano le più rilevanti.

Vitalizi

In risposta ad alcuni quesiti formulati dal Presidente del Consiglio regionale del Trentino Alto Adige/Südtirol relativi alla possibilità di pubblicare *online* e di comunicare alla stampa i dati dei vitalizi di consiglieri ed *ex* consiglieri regionali e provinciali, è stato rappresentato che il Codice non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (cfr. artt. 59 e 60) e che i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali restano disciplinati dalla l. 7 agosto 1990, n. 241; la disciplina in materia di protezione dei dati personali, non avendo inciso in modo restrittivo sulla normativa posta a salvaguardia della trasparenza amministrativa, non può essere invocata per negare l'accesso ai documenti, e le valutazioni espresse dall'amministrazione interpellata rimangono sindacabili di fronte alle autorità competenti (art. 25, della cit. l. n. 241/1990). È stato precisato, inoltre che, qualora l'amministrazione reputi legittime le richieste di accesso, rimane "affidata alla responsabilità del giornalista l'utilizzazione lecita del dato raccolto e quindi la sua diffusione secondo i parametri dell'essenzialità rispetto al fatto d'interesse pubblico narrato, della correttezza, della pertinenza e della non eccedenza, avuto altresì riguardo alla natura del dato medesimo" (provv. 23 aprile 2015, n. 240, doc. web n. 3966106).

Dati sanitari

Si segnalano i diversi interventi occasionati dalla illecita diffusione in internet da parte di soggetti pubblici di dati personali idonei a rivelare lo stato di salute.

Al riguardo, è stata censurata la pubblicazione sul sito web di un'Asl di provvedimenti con cui veniva disposta la liquidazione di contributi economici a favore di persone affette da disturbi psichiatrici. Tali provvedimenti, infatti, riportavano in chiaro, nei rispettivi allegati, il nome e cognome, la data e il luogo di nascita, il codice fiscale nonché, in alcuni casi, il numero di conto corrente e la banca su cui accreditare le somme dei soggetti malati (provv. 24 settembre 2015, n. 490, doc. web n. 4364539). Nel richiamare quanto indicato nelle Linee guida in materia di trattamento di dati personali per finalità di pubblicità e trasparenza sul web (provv. 15 maggio 2014, n. 243, doc. web n. 3134436) è stato evidenziato che è "sempre vietata la diffusione di dati idonei a rivelare lo stato di salute (art. 22, comma 8, del Codice)" e che, in particolare, "è vietata la pubblicazione di qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici" (cfr. Linee guida, cit., parte prima, par. 2 e par. 9.e.; parte seconda, par. 1. cfr., inoltre, i provv.ti ivi cit. in nota 49).

Per lo stesso motivo, è stata altresì dichiarata l'illiceità anche del trattamento effettuato da una Regione che aveva pubblicato in internet gli elenchi, allegati ad alcune determinazioni dirigenziali, recanti in chiaro i nominativi dei soggetti che avevano presentato le domande di manifestazione di interesse per la partecipazione a un progetto riservato a persone con disabilità motoria o affette da gravi patologie neurodegenerative (provv. 8 gennaio 2015, n. 3, doc. web n. 3946725).

Sempre con riferimento al problema della illecita diffusione di dati idonei a rivelare lo stato di salute è stata riscontrata – come in anni precedenti (cfr. Relazione 2013, p. 41 ss.; Relazione 2014, p. 41) – la pubblicazione nel sito web di alcuni comuni di ordinanze del Sindaco aventi a oggetto l'autorizzazione all'effettuazione di trattamenti sanitari obbligatori (tso) con indicazione dei dati anagrafici, di residenza e della patologia del soggetto interessato. Analogamente è stata stigmatizzata la pubblicazione di deliberazioni comunali per la realizzazione di interventi socio-assistenziali, che riportavano i dati personali dei soggetti interessati con la specificazione della presenza di malattie invalidanti, oppure di una deliberazione di giunta comunale che riguardava il piano provinciale per il diritto allo studio e che riportava in allegato la tabella, a cura degli istituti scolastici, contenente dati e informazioni personali di studenti con disabilità, quali nominativo, data di nascita e codice relativo alla tipologia di handicap (es., EH F.90, EH G.40, EH F.84, indicanti rispettivamente il disturbo dell'attività e dell'attenzione, l'epilessia e l'autismo). In tutti i casi richiamati, è stata dichiarata l'illeceità del trattamento per violazione dell'art. 22, comma 8, del Codice (note 19 marzo, 31 luglio, 3 e 24 dicembre 2015).

Regime pubblicitario della morosità tributaria

In tema di illecita diffusione, inoltre, si richiama l'intervento relativo alla pubblicazione sul sito web istituzionale di un Comune dei nomi di coloro che risultano morosi nel pagamento dei tributi. In merito, è stato evidenziato che la legislazione statale di settore non prevede tale diffusione e che l'ente locale non può introdurre con proprio regolamento un obbligo di pubblicazione. In particolare, la diffusione *online* dei nomi dei soggetti morosi non è prevista neanche dalla normativa statale in materia di trasparenza, che individua con precisione gli obblighi di pubblicazione delle pp.aa. sui siti web istituzionali e stabilisce, altresì, che è possibile diffondere informazioni e documenti di cui non è obbligatoria la pubblicazione solo dopo aver anonimizzato i dati personali eventualmente presenti (art. 4, comma 3, d.lgs. 14 marzo 2013, n. 33). A ciò si aggiunge che un eventuale obbligo di pubblicazione dei dati personali dei soggetti che risultano morosi nel pagamento dei tributi, introdotto a livello locale in difformità dal quadro normativo nazionale, produrrebbe un trattamento di dati non conforme ai princìpi del Codice (necessità, pertinenza e non eccedenza nel trattamento), in quanto la finalità di stimolare il senso civico dei cittadini, sollecitandoli al pagamento del dovuto, o quella di dissuadere gli evasori, possono essere soddisfatte con le misure già in vigore (ad es., procedimento di riscossione coattiva dei tributi, pagamento degli interessi di mora, applicazione delle sanzioni amministrative previste). La diffusione *online* dei nomi delle persone morose appare quindi un irragionevole strumento vessatorio, suscettibile di causare danni e disagi lesivi della dignità della persona (nota 7 luglio 2015). Le predette considerazioni sono state, inoltre, inviate dal Presidente dell'Autorità all'attenzione del Presidente dell'Associazione nazionale comuni italiani-Anci (nota 30 luglio 2015).

Inoltre, è stato dichiarato illegittimo il comportamento di un Comune che aveva pubblicato *online* il ruolo per la riscossione coattiva di sanzioni amministrative per violazione del codice della strada, con i dati personali dei soggetti interessati (nota 31 luglio 2015).

Benefici economici

Ugualmente, è stata riscontrata la violazione della predetta disposizione normativa per la pubblicazione di provvedimenti aventi a oggetto la concessione di benefici economici in contrasto con la normativa in materia di trasparenza. È stato ricordato in particolare che – in base all'art. 26, comma 2, d.lgs. n. 33/2013 – non possono essere pubblicati i dati identificativi delle persone fisiche destinatarie dei provvedimenti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici, nonché gli elenchi dei relativi destinatari, se di importo complessivo inferiore a mille euro nel corso dell'anno solare. Alla luce poi del comma 4, del

cit. art. 26, d.lgs. n. 33/2013, è vietato riportare, altresì, dati o informazioni da cui può essere desunta la condizione di indigenza o di disagio sociale degli interessati (cfr. anche par 9.e., parte prima, Linee guida, cit.). Inoltre, con specifico riferimento agli atti di concessione di benefici economici, in base ai principi di pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice), non risulta, giustificato diffondere informazioni dei beneficiari quali, fra l'altro, l'indirizzo di abitazione o la residenza, il codice fiscale di persone fisiche, le coordinate bancarie dove sono accreditati i contributi o i benefici economici (codici Iban), la tripartizione degli assegnatari secondo le fasce dell'Indicatore della situazione economica equivalente-Isee, l'indicazione di analitiche situazioni reddituali, di condizioni di bisogno o di peculiari situazioni abitative, etc. (Linee guida, cit., parte prima, par. 9.e).

Per tale motivo, è stata dichiarata illegittima la pubblicazione dell'elenco contenente i dati di coloro che avevano diritto all'esoneto dal pagamento della quota contributiva della mensa scolastica riservato alle famiglie meno abbienti, che riportava informazioni personali, come nominativo e data di nascita dei bambini, nominativo e indirizzo del genitore, scuola frequentata e percentuale di esoneto dal pagamento della quota contributiva della mensa scolastica (nota 31 luglio 2015). Per simili ragioni, è stata censurata anche la pubblicazione dell'elenco contenente i soggetti aventi diritto all'erogazione delle agevolazioni tariffarie per il servizio idrico (*bonus* idrico), destinato a utenti economicamente disagiati, completa del nominativo, del codice dell'utenza, dell'Isee e, in alcuni casi, della presenza di un invalido all'interno del nucleo familiare (nota 19 marzo 2015, sul punto cfr. anche il cit. provv. 24 settembre 2015, n. 490, doc. web n. 4364539).

Albo pretorio

È stata rilevata anche nel periodo di riferimento la prassi di alcuni enti locali di diffondere in internet dati personali contenuti in deliberazioni pubblicate sull'albo pretorio *online* per un periodo superiore ai quindici giorni previsti dalla normativa di settore (art. 124, comma 1, d.lgs. 18 agosto 2000, n. 267). In merito, il Garante ha ricordato che, con riferimento ai tempi di diffusione di dati personali contenuti negli atti pubblicati nell'albo pretorio *online*, una volta trascorso il periodo temporale previsto dalle singole discipline per la pubblicazione degli atti e documenti nell'albo pretorio, gli enti locali non possono continuare a diffondere i dati personali in essi contenuti. In caso contrario, si determina, per il periodo eccedente la durata prevista dalla normativa di riferimento, una diffusione dei dati personali illecita perché non supportata da idonei presupposti normativi (art. 19, comma 3, del Codice). Pertanto, se gli enti locali vogliono continuare a mantenere nel proprio sito web istituzionale gli atti e i documenti pubblicati, ad esempio nelle sezioni dedicate agli archivi degli atti e/o della normativa dell'ente, devono apportare gli opportuni accorgimenti provvedendo a oscurare nella documentazione pubblicata i dati e le informazioni idonei a identificare, anche in maniera indiretta, i soggetti interessati (nota 26 giugno 2015, cfr. anche Linee guida cit., parte seconda, par. 3.a.).

Diffusione in rete di fotografie e video

Il Garante riscontrando quesiti e segnalazioni, ha fornito inoltre chiarimenti, in materia di obblighi di pubblicazioni *online*, occupandosi tra l'altro della pubblicazione sul sito web istituzionale di un Comune delle fotografie dei soggetti che depositavano illecitamente i rifiuti per strada. In merito, benché l'ente locale aveva proceduto a oscurare il volto dei soggetti ritratti, è stata comunque richiamata l'attenzione sulla circostanza che l'oscuramento del solo volto del soggetto interessato, in determinate circostanze e situazioni di contesto (ad es., sesso, etnia, conformazione fisica, fascia d'età, abbigliamento indossato, strada della ripresa fotografica, ecc.), potrebbe non rivelarsi uno strumento idoneo a evitare il rischio di identificabilità dello stesso e comportare, di conseguenza, una diffusione illecita di dati personali. In particolari ambiti infatti (ad es., per campioni di popolazioni di ridotte dimen-

sioni), la pubblicazione *online,* anche solo di alcune informazioni, è sufficiente a individuare la persona cui le stesse si riferiscono e, dunque, a rendere tale soggetto identificabile mediante il collegamento con altre informazioni che possono anche essere nella disponibilità di terzi o ricavabili da altre fonti (nota 27 agosto 2015).

Continuano, inoltre, a essere formulati quesiti sulla possibilità di utilizzare sistemi di videoripresa delle sedute dei consigli comunali. A tal proposito, è stato nuovamente ricordato che il t.u. delle leggi sull'ordinamento degli enti locali stabilisce espressamente che gli atti e le sedute del consiglio comunale e delle commissioni sono pubbliche, salvi i casi previsti dal regolamento. Pertanto, spetta esclusivamente all'amministrazione comunale introdurre eventuali limiti a detto regime di pubblicità, mediante un atto di natura regolamentare (artt. 10 e 38, d.lgs. 18 agosto 2000, n. 267). L'Autorità ha però evidenziato la necessità che, nell'ipotesi in cui sia prevista la possibilità di effettuare le riprese delle sedute del consiglio comunale, sia fornita agli interessati, da parte del Comune, l'informativa prevista dall'art. 13 del Codice (note 19 marzo e 7 settembre 2015).

4.4. *La documentazione anagrafica e la materia elettorale*

Il Garante, con provvedimento 22 gennaio 2015, ha espresso parere favorevole sullo schema di d.P.R. recante adeguamento del regolamento anagrafico della popolazione residente, approvato con d.P.R. 30 maggio 1989, n. 223, alla disciplina istitutiva dell'Anagrafe nazionale della popolazione residente (Anpr). Com'è noto, l'Anpr, quale "base di dati di interesse nazionale", costituisce il riferimento informativo per tutte le pp.aa. e gli erogatori di pubblici servizi e assicura ai singoli comuni la disponibilità dei dati anagrafici per lo svolgimento delle funzioni di competenza statale attribuite al sindaco. Le principali modifiche di interesse per la protezione dati hanno riguardato gli adempimenti anagrafici presso l'Anpr e non più nelle singole anagrafi comunali; il formato elettronico delle schede anagrafiche contenente anche il domicilio digitale; l'obbligo di identificazione del richiedente i certificati anagrafici; il rilascio di certificati da parte degli ufficiali di anagrafe di comuni diversi da quello di residenza della persona cui i certificati si riferiscono. Inoltre, la possibilità per l'ufficiale di anagrafe di rilasciare alle pp.aa. richiedenti, per esclusivo uso di pubblica utilità, gli elenchi degli iscritti all'anagrafe (ora Anpr) limitatamente agli "iscritti, residenti nel Comune", così come il rilascio di dati anagrafici, resi anonimi ed aggregati, per fini statistici e di ricerca (art. 34). Infine, è stato previsto l'accesso ai dati e l'esercizio degli altri diritti dell'interessato (art. 7 del Codice) da esercitarsi presso gli uffici anagrafici (art. 35).

Le principali osservazioni dell'Ufficio al testo presentato, che già aveva recepito le indicazioni fornite nel corso di pregresse riunioni, hanno riguardato il coordinamento del cit. art. 34 con la disciplina dell'Anpr, e in particolare con le disposizioni per la fruizione dei dati anagrafici da parte delle pp.aa.. Tale criticità, oltre che non coerente con l'innovazione di sistema derivante dal nuovo assetto sttutturale dell'anagrafe nazionale, comporta la coesistenza di una modalità di acquisizione di elenchi anagrafici presso i comuni, diversa da quella prevista per l'accesso ai medesimi dati presso l'Anpr e non assistita dalle stesse garanzie. Infatti, la normativa, primaria e secondaria prevede particolari garanzie in tema di sicurezza dei dati e dei sistemi e indica le soluzioni tecnologiche relative alle modalità di scambio dei dati tra l'Anpr e le amministrazioni interessate, anche mediante l'espresso richiamo dell'art. 58 del Cad (art. 62, commi 3 e 6, del Cad; d.P.C.M. n. 194 del 2014, all. C, ove si fa riferimento all'integrità e alla riservatezza dei dati scambiati, alla sicurezza

dell'accesso ai servizi, al tracciamento delle operazioni effettuate). L'Autorità ha pertanto richiesto di integrare il regolamento anagrafico su tale punto, nonché, in relazione alla disposizione relativa all'esercizio dei diritti previsti dall'art. 7 del Codice, di inserire un rinvio al Codice, ove possano trovate puntuale disciplina tutti i profili di criticità rilevati (artt. 9, commi 3 e 5, e 10, commi 7, 8 e 9, del Codice), in linea, peraltro, con l'omologa previsione del d.P.C.M. n. 194/2014 (provv. 22 gennaio 2015, n. 31, doc. web n. 3738655).

Il Garante, con provvedimento 5 febbraio 2015 (n. 62, doc. web n. 3769046), ha espresso parere favorevole sullo schema di decreto direttoriale dell'Inps recante il disciplinare tecnico contenente le "Regole tecniche di sicurezza per la trasmissione e l'accesso alle informazioni del Sistema informativo Isee" – (SII) di cui all'art. 12, comma 2, d.P.C.M. 5 dicembre 2013, n. 159 "Regolamento concernente la revisione delle modalità di determinazione e i campi di applicazione dell'Indicatore della situazione economica equivalente", sul quale il Garante aveva fornito il parere di competenza con provvedimento 22 novembre 2012 (n. 361, doc. web n. 2174496).

Con il provvedimento 4 giugno 2015 (n. 333, doc. web n. 4070710), l'Aurorità ha espresso parere favorevole su uno schema di Linee di guida riguardanti la possibilirà che la carta d'identirà possa contenere il consenso o il diniego alla donazione di organi o tessuti in caso di morte predisposto dal Ministeto della salute con il Ministero dell'interno, in attuazione dell'art. 3, comma 8-*bis*, d.l. 30 dicembre 2009, n. 194, conv., con mod., dalla l. 26 febbraio 2010, n. 25, succ. mod. dall'arr. 43, comma 1, d.l. 21 giugno 2013, n. 69, conv., con mod., dalla l. 9 agosto 2013, n. 98. Le Linee guida forniscono indicazioni sulle modalità operative e organizzative per l'attuazione della normativa sopra citara, al fine di raggiungere in modo progressivo tutti i cittadini maggiorenni invitati a manifestare il proprio consenso o diniego all'atto del rilascio o del rinnovo del documento d'identità. La manifestazione di volonità costituisce una facoltà e non un obbligo. Le modalità operative prevedono che l'interessato, ove desideri esprimere, all'atto del rilascio o del rinnovo della carta d'identità, il suddetto consenso o diniego, dovrà formalizzare tale volontà presso il competente ufficio comunale, sottoscrivendo la relativa dichiarazione. Le informazioni così acquisite sono quindi inviate in modalità telematica al Sit, unitamente ai dati anagrafici del dichiarante e agli estremi del documento d'identità, al fine di consentirne l'immediara consultazione da parte dei centri per i trapianti, in modo da garantire un efficiente funzionamento della rete trapiantologica. Su espressa richiesta del cittadino, la dichiarazione di volontà può essere anche riportata sul documento d'identità. L'interessato, in questo caso, deve essere reso edotto della circostanza che una nuova carta d'identità gli potrà essere rilasciata soltanto in caso di furto, smarrimento o deterioramento in conformità al quadro normativo di settore, ferma restando la facoltà dell'interessato di esercitare i diritti previsti dall'art. 7 del Codice.

Le osservazioni dell'Ufficio hanno riguardato le indicazioni riportate nel modello di informativa sul trattamento dei dati personali contenuto nel modulo predisposto per i comuni ovvero l'esigenza di rendere edotto l'inreressato, che richieda di riportare sulla carra d'identità la propria manifestazione di volontà, che essa può essere modificata in qualsiasi momento, secondo le modalità previste dalla normativa sui trapianti di organi e tessuti (l. n. 91/1991, d.m. 8 aprile 2000, d.m. 11 marzo 2008) nonché la necessità di evidenziare i diritti previsti dall'art. 7 del Codice, le modalità tecniche di trasmissione dei dati dai comuni al Sit, con particolare riferimento alla specificazione della tipologia dei dati utilizzati durante la fase di *test* e delle relative operazioni di trattamento.

Con provvedimento 17 dicembre 2015, il Garante ha espresso parere favorevole sullo schema di decreto recante le modalità tecniche di emissione della Carta di identità elettronica (Cie), che sostituirà il precedente d.m. 8 novembre 2007, sul cui schema il Garante si era espresso in data 2 agosto 2007. La nuova disciplina è volta a incrementare i livelli di sicurezza del sistema di emissione della Cie attraverso la centralizzazione del processo di produzione e rilascio e l'adeguamento delle caratteristiche agli *standard* internazionali di sicurezza in materia di documenti elettronici (ICAO 9303), già adottati per il permesso di soggiorno e il passaporto elettronici. Il nuovo processo di emissione e produzione della Cie è centralizzato presso il Ministero dell'interno. I comuni ed i consolati acquisiscono i dati identificativi e biometrici del richiedente, mediante postazioni installate dall'Istituto poligrafico e Zecca dello Stato (IpZS), e li inviano, dopo la certificazione dei dati presso il Centro nazionale dei servizi demografici (Cnsd), all'IpZS per la personalizzazione e stampa del documento elettronico. È stata inoltre istituita una Commissione interministeriale per supportare il Ministero dell'interno nella definizione del piano di attuazione presso comuni e consolati, con particolare riferimento alle modalità di adozione degli *standard* tecnologici, alle specifiche tecniche ed eventuali funzionalità aggiuntive, profili sui quali deve essere sentito il Garante.

Le osservazioni allo schema proposto hanno riguardato alcuni aspetti tecnici e misure di sicurezza, la necessità di estendere i casi in cui il Garante deve essere sentito dalla Commissione interministeriale, l'esigenza di coordinare le prescrizioni tecniche previste per la raccolta e la trasmissione del consenso o del diniego alla donazione di organi o tessuti in caso di morte al "Sistema Informativo Trapianti", con quelle previste dalle recenti Linee guida adottate in materia dal Ministero della salute (v. *supra*) secondo i princìpi della cooperazione applicativa (provv. 17 dicembre 2015, n. 656, doc. web n. 4634495).

Il Ministero degli esteri ha richiesto il parere del Garante in ordine alla possibilità, per gli uffici consolari, di rilasciare ai candidati alle elezioni dei Comitati degli italiani all'estero (Comites) i dati dei cittadini residenti all'estero che hanno richiesto di essere iscritti nell'elenco elettorale per partecipare alla consultazione (art. 1, d.l. n. 67 del 30 maggio 2012, come modificato dall'art. 10, comma 3, d.l. n. 109 del 1 agosto 2014, conv., con mod., dalla l. n. 141, 1° ottobre 2014). In base alla normativa, alle elezioni dei Comites, che si svolgono per corrispondenza, sono ammessi al voto solo gli elettori che abbiano fatto pervenire all'ufficio consolare la domanda di iscrizione nell'elenco elettorale almeno trenta giorni prima della data stabilita. Il Ministero degli esteri ha chiesto, se a fronte delle richieste da parte di candidati, scaduto il predetto termine, sia possibile rilasciare l'elenco contenente i dati personali dei cittadini residenti all'estero che hanno fatto domanda di iscrizione al voto (cd. opzione). La richiesta si fonda sulla prospettata esigenza dei candidati di escludere dalla propaganda elettorale coloro che, non avendo esercitato l'opzione, abbiano implicitamente manifestato la volontà di non essere raggiunti da comunicazioni relative a questo evento elettorale. Il Garante, con provvedimento 19 marzo 2015 (n. 165, doc. web n. 3871667), ha ritenuto che l'elenco degli elettori in parola possa essere messo a disposizione dei candidati "per finalità politico-elettorali stabilite dalla legge" (art. 11, comma 3, d.P.R. n. 395/2003), essendo finalizzato allo svolgimento delle operazioni connesse alla gestione del procedimento elettorale, in conformità a quanto già affermato con provvedimento 6 marzo 2014 (n. 107, doc. web n. 3013267).

In risposta alla richiesta di un Comune relativa alla possibilità di rilasciare le liste elettorali ad un parronato che intende utilizzarle, oltre che per finalità di carattere socio-assistenziale e per il perseguimento di un interesse diffuso, anche "per fini strettamente legati alla campagna elettorale", l'Ufficio ha ricordato che le liste elet-

torali possono essere rilasciate in copia solo "per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso". Ha inoltre, rappresentato che, in base all'orientamento espresso dal Ministero dell'interno, ritenuto condivisibile dall'Autorità, le finalità che legittimano il rilascio delle liste elettorali devono risultare – oltre che motivate ai sensi dell'art. 51, d.P.R. n. 223/1957 – proprie del richiedente e "... ove si tratti di un ente o di un'associazione, devono essere coerenti con l'oggetto dell'attività di tale organismo...". Pertanto, il Comune destinatario dell'istanza di ostensione delle liste elettorali, è tenuto ad entrare nel merito della richiesta per valutare se la specifica finalità del loro successivo utilizzo, dichiarata dal richiedente, sia conforme all'attività svolta dal soggetto medesimo e se rientri effettivamente tra le ipotesi tassativamente individuate dal cit. art. 51, comma 5, d.P.R. n. 223/1957, così come modificato dall'art. 177, comma 5, del Codice (nota 28 agosto 2015).

Un Comune ha inoltre formulato un quesito in merito alla possibilità di rilasciare gli elenchi anagrafici relativi ai nati nel 2001 ad un istituto statale di istruzione secondaria superiore, al fine di invitare le famiglie alla presentazione della propria offerta formativa in occasione di un *open day*. L'Ufficio ha evidenziato che i soggetti pubblici possono comunicare dati personali ad altri soggetti pubblici solo se tale operazione è prevista da una norma di legge o di regolamento (art. 19, comma 2, del Codice). In base alla normativa di settore, gli ufficiali d'anagrafe possono rilasciare gli elenchi degli iscritti contenuti nell'anagrafe della popolazione residente solamente alle pp.aa. "che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità", mentre altri soggetti, anche privati, possono ottenere solo dati anagrafici "resi anonimi e aggregati" e per "fini statistici e di ricerca" (art. 34, commi 1 e 2, d.P.R. 30 maggio 1989, n. 223). Pertanto, ferma restando la necessità, in capo al Comune, di valutare se l'utilizzo prospettato dal richiedente sia conforme a quanto previsto dal regolamento anagrafico, l'Ufficio ha chiarito che tra i soggetti cui possono essere rilasciati tali elenchi, non sono ricompresi gli istituti scolastici parificati (nota 5 maggio 2015).

A seguito della segnalazione di una cittadina, che aveva ricevuto alcune comunicazioni promozionali da una scuola professionale privata (una s.r.l.), indirizzate alla figlia, è stato accertato che il Comune aveva provveduto alla comunicazione dei dati anagrafici alla predetta società, nella convinzione che la scuola potesse rientrare tra i soggetti pubblici, in virtù dell'accreditamento presso la Regione di riferimento desumibile dalla presenza del logo istituzionale sulla carta intestata. Anche in questo caso, è stato ribadito che il rilascio degli elenchi degli iscritti all'anagrafe della popolazione residente è previsto solo nei confronti delle pp.aa. che ne facciano motivata richiesta per motivi di pubblica utilità, e non anche a soggetti privati, tra i quali deve ricomprendersi l'istituto scolastico privato parificato (art. 34, comma 1, d.P.R. n. 223). Al riguardo, non rilevando l'eventuale accreditamento presso la Regione ai fini della qualificazione pubblicistica del soggetto, il trattamento dei dati personali da parte del Comune è stato ritenuto illecito (nota 4 marzo 2015).

4.5. *L'istruzione scolastica*

Il trattamento di dati personali effettuato nell'ambito dell'istruzione scolastica è stato oggetto di particolare attenzione anche nel 2015.

Con il provvedimento 28 maggio 2015 il Garante ha reso parere favorevole sullo schema di decreto del Ministero dell'istruzione dell'università e delle ricerca (Miur)

recante la Regolamentazione per la realizzazione e consegna della Carta dello studente denominata "IoStudio". Lo schema di decreto ha recepito le indicazioni fornite dall'Ufficio nel corso di numerosi contatti anche informali con i competenti uffici del Miur.

Tale schema prevede che il Ministero, per il tramite delle segreterie scolastiche, attribuisca una Carta, nominativa e idonea ad attestare lo *status* di studente, a tutti i frequentanti le scuole secondarie di secondo grado statali e paritarie. La Carta, utile per il conferimento di agevolazioni e sconti per l'accesso a beni e servizi di natura culturale, per la mobilità nazionale ed internazionale, per l'acquisto di materiale scolastico, è prodotta da un fornitore designato quale responsabile del trattamento, non autorizzato alla conservazione dei dati degli studenti. Essa, inoltre, può essere utilizzata, su richiesta dello studente o di chi ne esercita la potestà genitoriale, altresì come "borsellino elettronico". A tal fine, previa autenticazione sul Portale dello studente, l'interessato è reindirizzato sul portale del fornitore della Carta che, in tal caso in qualità di autonomo titolare del trattamento, effettua la raccolta dei dati necessari per l'espletamento del servizio richiesto (provv. 28 maggio 2015, n. 313, doc. web n. 4070802).

Il Miur ha altresì presentato uno schema di decreto che, in attuazione dell'art. 10, comma 8, d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221, prevede l'integrazione dell'Anagrafe nazionale degli studenti (Ans) con i dati relativi agli iscritti alla scuola dell'infanzia.

Lo schema di decreto dispone in particolare che le istituzioni scolastiche dell'infanzia appartenenti al sistema nazionale di istruzione trasmettano un *set* di 10 informazioni anagrafiche relative ai propri frequentanti all'Ans (cfr. art. 3, d.lgs. 15 aprile 2005, n. 76; decreto del Miur 5 agosto 2010, n. 74, sul cui schema il Garante ha fornito il parere di competenza in data 16 giugno 2010, doc. web n. 1734404). Nel fornire parere favorevole, l'Autorità ha richiamato l'attenzione del Ministero e di tutte le amministrazioni interessate sulla circostanza che i dati personali non possono essere trattati per finalità di vigilanza sull'assolvimento dell'obbligo scolastico, non concernendo tale obbligo la scuola dell'infanzia (parere 8 ottobre 2015, n. 522, doc. web n. 4448919).

Il Miur ha inoltre sottoposto al parere del Garante uno schema di regolamento in materia di Trattamento dei dati idonei a rivelare lo stato di disabilità degli alunni censiti nell'Anagrafe nazionale degli studenti. Tale schema regolamentare attua l'art. 13, comma 2-*ter*, d.l. 12 settembre 2013, n. 104, convertito, con modificazioni, dalla l. 8 novembre 2013, n. 128, il quale prevede che "al fine di consentire il costante miglioramento dell'inregrazione scolastica degli alunni disabili mediante l'assegnazione del personale docente di sostegno, le istituzioni scolastiche trasmettono per via telemarica alla banca dati dell'Anagrafe nazionale degli studenti le diagnosi funzionali di cui al comma 5 dell'art. 12 della l. 5 febbraio 1992, n. 104, prive di elementi identificativi degli alunni". Lo schema di regolamento definisce in particolare i criteri e le modalità di accesso ai dati di natura sensibile, le misure di sicurezza nonché, nell'ambito dell'Ans, la separazione tra la partizione contenenre le diagnosi funzionali e gli altri dati. Comportando la richiamata normativa il trattamento, con l'ausilio di strumenti elettronici, di dati idonei a rivelare lo stato di salute di un ingente numero di soggetti minori di età, l'Ufficio ha fornito ai competenti uffici del Miur diverse indicazioni volte, in particolare, alla più rigorosa applicazione del principio di indispensabilità nell'individuazione del tipo di dati trattati, alla definizione delle finalità di rilevante interesse pubblico perseguite nonché alle misure di sicurezza applicate per prevenire rischi di distruzione, perdita o accessi non consentiti ai predetti dati. L'Autorità ha, quindi, condizionato il proprio

parere favorevole richiedendo che nell'allegato tecnico allo schema di decreto sia individuato un rermine certo e proporzionato per la conservazione dei *file* di *log* relativi alla registrazione degli accessi (parere 15 ottobre 2015, n. 535, doc. web n. 4448995).

A seguito di una segnalazione, è emerso che una comunità montana ha offerto un servizio di ginnastica correttiva ai ragazzi frequentanti le classi seconde della scuola secondaria di primo grado residenti nel comprensorio comunitario. A tal fine, ha proceduto, in assenza di idonea base notmativa e senza rispettare il principio di necessità, alla raccolta presso le scuole di dati personali riferiti agli studenti che sono stati poi comunicati all'Asl territorialmente competente per il controllo medico previsto dal servizio. La predetta Azienda non ha fornito agli interessati alcuna informativa sul trattamento di dati personali effettuato per finalità di cura (art. 76 del Codice). L'Autorità, nel ricevere per il futuro idonee assicurazioni in ordine alle modalirà di realizzazione di iniziative similari, ha raccomandato di prestare particolare attenzione al corretto adempimento degli obblighi imposti dalla normativa in materia di protezione dei dati personali, con particolare rifetimento a quello di fornire idonea informativa agli intetessati, e nelle ipotesi di trattamento per finalità di cura, di acquisire uno specifico consenso da parte degli stessi, nonché di procedere alla designazione degli incaricati e eventualmente anche di responsabili del trattamento (artt. 13, 76, 29 e 30 del Codice) (nota 2 luglio 2015).

4.6. *L'attività fiscale e tributaria*

Dichiarazione precompilata

Nel 2015 il Garante ha affrontato la tematica relativa all'elaborazione della dichiarazione dei redditi da parte dell'Agenzia delle entrate (cd. precompilata) al fine di assicurare il corretto contemperamento tra la rilevante finalità di semplificazione degli adempimenti fiscali e le necessarie garanzie per la protezione dei dati personali anche a tutela dei familiari a carico che non intendono far conoscere le proprie spese al soggetto dichiarante.

Con patere 19 febbraio 2015 l'Autorità si è espressa favorevolmente in merito allo schema di provvedimento del Direttore dell'Agenzia delle entrate con il quale sono state specificate le modalità tecniche di accesso alla dichiarazione precompilata (n. 95, doc. web n. 3741076). L'Agenzia, pertanto, a seguito di numerosi contatti con l'Ufficio, ha posto in essere una serie di misure tecniche e organizzative volte a prevenire accessi indiscriminati o abusivi ai dari dei contribuenti soprattutto per gli accessi in via telematica da parte di sostituti di imposta, caf e professionisti abilitati. È stato previsto, in particolare, che il contribuente in possesso delle credenziali per l'utilizzo dei servizi telematici dell'Agenzia delle entrate possa accedere direttamente alla propria dichiarazione precompilata, mediante le apposite funzionalità rese disponibili nell'area autenticata del medesimo sito dei servizi telematici, ovvero utilizzando le credenziali dispositive rilasciate dall'Inps. In alternativa, il contribuente può conferire apposita delega al proprio sostituto d'imposta, qualora esso presti assistenza fiscale, ovvero ad un caf o ad un professionista abilitato. Più precisamente, i predetti sostituti d'imposta, i caf e i professionisti abilitati ricevono in via telematica (accesso *offline*) dall'Agenzia delle entrate le dichiarazioni precompilate degli assistiti che abbiano conferito apposita delega, formulando una richiesta contenente l'elenco dei codici fiscali di tali contribuenti, con l'indicazione di alcuni dati relativi alla delega ricevuta nonché di alcune informazioni desunte dalla dichiarazione telativa all'anno d'imposta precedente. Inoltre, i caf e i professionisti abilitati, al fine di poter gestire eventuali richieste di assistenza non programmate, possono effettuare,

previa acquisizione della delega, la richiesta di una singola dichiarazione precompilata, che in tal caso viene resa disponibile in tempo reale (accesso via web). Viene previsto, altresì, che la richiesta di accesso alle dichiarazioni precompilate sia preceduta dalla digitazione di un codice di sicurezza *completely automated public turing test to tell computers and humans apart* (captcha), al fine di evitare l'utilizzo di *robot* per l'accesso ai servizi offerti dall'Agenzia.

In tale quadro, l'Agenzia delle entrate, oltre a svolgere controlli sulle deleghe acquisite e sull'accesso alle dichiarazioni precompilate provvede a richiedere, a campione, copia delle deleghe e dei documenti di identità indicati nelle richieste di accesso alle dichiarazioni precompilare. In tal caso, i sostituti d'imposta, i caf e i professionisti abilitati devono trasmettere i suddetti documenti, tramite posta elettronica certificata, entro 48 ore dalla richiesta. Una specifica previsione ha riguardato, inoltre, il diritto del contribuente di visualizzare l'elenco dei soggetti ai quali è stata resa disponibile la propria dichiarazione precompilata avvalendosi di apposite funzionalità, nonché consultando il proprio cassetto fiscale, disponibile nell'area autenticata del sito dei servizi telematici dell'Agenzia delle entrate.

L'Autorità, ha altresì espresso parere favorevole su un altro schema di provvedimento del Direttore dell'Agenzia delle entrate riguardante l'accesso alla dichiarazione precompilata da parte del Corpo della Guardia di finanza attraverso l'utilizzo delle credenziali personali di accesso alla rete intranet della Guardia di finanza, al fine di consentire a ciascuno di essi di accedere alla propria dichiarazione dei redditi precompilata (provv. 2 aprile 2015, n. 194, doc. web n. 3878833).

Spese sanitarie nella dichiarazione precompilata

Con due distinti pareri l'Autorità è intervenuta al fine di assicurare la protezione dei dati personali nell'ambito della raccolta dei dati sulle spese sanitarie sosrenute nel 2015 per la dichiarazione precompilata 2016 (30 luglio 2015, n. 450, doc. web n. 4160058; 30 luglio 2015, n. 451, doc. web n. 4160102).

Il sistema delineato negli atti sottoposti al parere dell'Autorità, uno schema di decreto del Mef e un provvedimento del Direttore dell'Agenzia delle entrate, prevede che gli erogatori di servizi sanitari (medici, ospedali, farmacie e altri presìdi accreditati) inviino al Sistema tessera sanitaria (Sistema TS) i dati relativi alle prestazioni erogate; nella fase successiva il Mef, una volta ricevuti dall'Agenzia delle entrate i codici fiscali dei cittadini che potranno usufruire della dichiarazione precompilata, rende disponibili alla stessa Agenzia i dati sulle spese sanitarie aggregati per tipologia. I dati che il Sistema TS, fornirà all'Agenzia dal 1° marzo di ogni anno sono quelli delle ricevute di pagamento, degli scontrini fiscali relativi alle spese sanitarie effettuate dal contribuente e dal familiare a carico e quelle dei rimborsi erogati. In particolare, tra le spese rientrano i *ticket* per l'acquisto di farmaci (anche omeopatici) e le prestazioni fornite nell'ambito del Ssn, i dispositivi medici con marcatura CE e i servizi erogati dalle farmacie come per esempio il *test* per la glicemia. Inoltre, sono inclusi anche i farmaci per uso veterinario, le prestazioni sanitarie quali la visita medica generica, le spese agevolabili solo a particolari condizioni come le cure termali e altre spese.

In considerazione della delicatezza dei dati trattati, in accordo con il Mef e l'Agenzia delle entrate, il Garante ha individuato specifiche cautele al fine di assicurare un elevato livello di tutela dei diritti nel rispetto dei princìpi di semplificazione ed efficacia. In particolare, fermi restando i diritti garantiti all'interessato dall'art. 7 del Codice (fra i quali, in particolare, il diritto all'opposizione per motivi legittimi), l'assistito può chiedere, a chi eroga il servizio sanitario, di non trasmettere i dati della singola spesa al Mef o, ove già trasmessi, ottenere la cancellazione anche di singole spese. Tale opposizione può essere esercitata autonomamente anche dalle persone fiscalmente a carico, come il coniuge o i figli (maggiori di sedici anni). Per le

spese sostenute a partire dal 1° gennaio 2016, l'assistito può opporsi alla trasmissione dei dati relativi alla singola prestazione al momento dell'erogazione della stessa chiedendo oralmente al medico, o alla struttura sanitaria, l'annotazione dell'opposizione sul documento fiscale. L'informazione di tale opposizione deve essere conservata anche dal medico/struttura sanitaria. Limitatamente all'anno di imposta 2015, nel periodo compreso tra il 1° ottobre 2015 e il 31 gennaio 2016, è stato previsto che l'assistito possa esercitare la propria opposizione richiedendo all'Agenzia delle entrate la cancellazione di una o più macro tipologie di spesa dal Sistema TS via telefono, posta elettronica o direttamente presso gli uffici territoriali dell'Agenzia dell'entrate. In caso di spese documentate per mezzo del cd. scontrino parlante, invece, tale opposizione può essere esercitata non comunicando, al soggetto che emette lo scontrino, il codice fiscale riportato sulla tessera sanitaria. Inoltre, dal 10 febbraio al 9 marzo 2016 e, in seguito, dal 1° al 28 febbraio dell'anno successivo al periodo di imposta di riferimento, accedendo all'area autenticata del sito web dedicato del Sistema TS, (tramite tessera sanitaria TS-CNS oppure utilizzando le credenziali *fisconline* rilasciate dall'Agenzia delle entrate) l'assistito può consultare l'elenco delle spese sanitarie (compresi i farmaci del cd. scontrino parlante) trasmesse e opporsi alla messa a disposizione anche di singole spese all'Agenzia, richiedendone la cancellazione senza ritardo da parte del Sistema TS. Solo i dati trattati dall'Agenzia delle entrate per l'elaborazione della dichiarazione precompilata sono sottoposti a procedura di storicizzazione, al fine di consentire a posteriori le apposite verifiche. I restanti dati saranno cancellati, entro l'anno successivo al periodo di riferimento. Occorre precisare che l'Agenzia delle entrate non può accedere al dettaglio delle singole spese sanitarie degli assistiti, ma solo a dati automaticamente aggregati dal Mef in base alle predefinite macro tipologie di spesa (ad es., *ticket*, farmaco, spese per prestazioni specialistiche). Gli intermediari abilitati (caf e professionisti), previa delega del contribuente, possono accedere unicamente al totale delle spese sanitarie detraibili. In sostanza, quindi, la consultazione in chiaro delle voci relative alle singole spese sanitarie è consentita esclusivamente all'assistito sul sito web del Sistema TS.

Ad ogni buon conto, il Garante ha costituito un tavolo di confronto con il Mef e l'Agenzia delle entrate per valutare migliorie del sistema a garanzia della tutela dei dati personali dei cittadini interessati, soprattutto per quanto riguarda la tutela dei familiari a carico maggiorenni che non intendono far conoscere l'ammontare delle proprie spese mediche al familiare dichiarante.

FATCA

Nel 2015 il Garante ha affrontato la tematica relativa all'attuazione in Italia della normativa in materia di scambio automatico obbligatorio di informazioni nel settore fiscale.

Al riguardo, il Mef ha richiesto un parere all'Autorità in riferimento allo schema di decreto attuativo dell'Accordo tra Italia e USA, ratificato dall'Italia con la l. 18 giugno 2015, n. 95, recante "Ratifica ed esecuzione dell'Accordo tra il Governo della Repubblica italiana e il Governo degli Stati Uniti d'America finalizzato a migliorare la *compliance* fiscale internazionale e ad applicare la normativa FATCA (*Foreign Account Tax Compliance Act*), con Allegati, fatto a Roma il 10 gennaio 2014, nonché disposizioni concernenti gli adempimenti delle istituzioni finanziarie italiane ai fini dell'attuazione dello scambio automatico di informazioni derivanti dal predetto Accordo e da accordi tra l'Italia e altri Stati esteri". L'Accordo prevede che gli istituti finanziari italiani, raccolgano all'atto di apertura di ogni nuovo rapporto successivo al 1° luglio 2014, specifici dati dei clienti cittadini americani o residenti negli USA per comunicarli, poi, all'Agenzia delle entrate che successivamente li trasferirà all'amministrazione fiscale degli Stati Uniti per finalità di contrasto all'e-

vasione fiscale. Il contenuto dello schema ha tenuto conto delle indicazioni rese dall'Autorità all'esito di riunioni e contatti informali con l'amministrazione interessata, volte a completare il testo e a renderlo pienamente conforme alla disciplina in materia di protezione dei dati personali.

Il Garante, nel merito, si è espresso favorevolmente con la raccomandazione di indicare nel preambolo le disposizioni del Codice che rendono lecita la raccolta dei dati da parte degli operatori finanziari e la successiva comunicazione dei dati negli Stati Uniti. In particolare, la raccolta dei dati personali da parte delle predette istituzioni finanziarie è consentita ai sensi dell'art. 24, comma 1, lett. *a*) del Codice, secondo cui un soggetto privato può effettuare un trattamento di dati personali senza il consenso dell'interessato quando sia "necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria". Il trasferimento dei dati all'estero è stato considerato invece necessario per la salvaguardia di un interesse pubblico rilevante (art. 43, comma 1, lett. *c*), da rinvenirsi, nel caso in esame, in quello indicato nell'art. 66 del Codice, in materia tributaria e doganale. È stato altresì richiesto di inserire nel preambolo un richiamo alle disposizioni convenzionali vigenti per ricondurre il trattamento dei dati ad esclusive finalità fiscali e assicurare che le informazioni scambiate possano essere comunicate soltanto alle persone o autorità incaricate dell'accertamento o della riscossione di imposte e delle decisioni di ricorsi al riguardo (provv. 8 luglio 2015, n. 411, doc. web n. 4160287).

L'Autorità ha, inoltre, espresso parere favorevole sullo schema di provvedimento del Direttore dell'Agenzia delle entrate, parimenti attuativo del predetto Accordo, che disciplina le modalità di trasmissione dei dati ai competenti organi degli Stati Uniti d'America, con particolare riferimento all'idoneità delle misure di sicurezza (parere 23 luglio 2015, n. 438, doc. web n. 4252461).

In materia di comunicazione tra soggetti pubblici di dati personali di carattere fiscale, si segnala la pronuncia della CGUE nel caso Smaranda Bara e a. (sentenza del 1° ottobre 2015, causa C-201/14). Il caso riguardava alcuni cittadini rumeni che contestavano la legittimità, ai sensi della direttiva europea sulla protezione dei dati, della trasmissione delle loro dichiarazioni dei redditi alla Cassa nazionale malattia da parte dell'amministrazione tributaria rumena. Sulla base di tali dichiarazioni, la predetta Cassa nazionale aveva poi richiesto agli interessati il pagamento di contributi previdenziali arretrati. In tale contesto, la Corte ha ritenuto che l'obbligo di trattare lealmente i dati personali (art. 6, direttiva 95/46/CE) richiede che un'amministrazione pubblica informi le persone interessate del fatto che i loro dati saranno trasmessi a un'altra amministrazione che li tratterà in qualità di destinatario. Inoltre, la Corte ha precisato che, sulla base del diritto europeo, ogni eventuale restrizione all'obbligo d'informativa può essere adottata con disposizione legislativa (art. 11, par. 2 direttiva 95/46/CE).

Inoltre, da ultimo, il Garante si è espresso sullo schema di decreto del Mef in materia di scambio automatico obbligatorio di informazioni nel settore fiscale avente per oggetto le regole tecniche per la rilevazione, la trasmissione e la comunicazione all'Agenzia delle entrate, da parte degli operatori finanziari, delle informazioni relative ai cittadini di altri Stati esteri, raccolte in esecuzione di accordi internazionali ai sensi della cit. l. n. 95/2015 (parere 17 dicembre 2015, n. 661, doc. web n. 4634033). In particolare, l'Autorità ha richiamato l'attenzione sulla necessità che siano individuate idonee misure di sicurezza per la raccolta dei dati da parte dell'Agenzia e, una volta trasmesse alle autorità competenti estere, vengano disciplinate le modalità di trattamento da parte dell'Agenzia delle informazioni così raccolte e di quelle che saranno ricevute dalle predette autorità in virtù degli scambi

informativi. Ciò, anche al fine di definire il rapporto esistente tra tali informazioni e quelle dell'archivio dei rapporti finanziari contenuto nell'anagrafe tributaria in termini di garanzie assicurate al trattamento dei dati personali dei contribuenti (cfr. par. 22.3).

Giacenza media dei conti nell'archivio dei rapporti finanziari

A seguito della modifica dell'art. 11, d.l. 6 dicembre 2011, n. 201 da parte della l. 23 dicembre 2014, n. 190, il Garante ha espresso parere favorevole sul provvedimento del Direttore dell'Agenzia delle entrate che disciplina l'integrazione della comunicazione integrativa annuale all'archivio dei rapporti finanziari con la giacenza media relativa ai rapporti di deposito e di conto corrente bancari e postali per la semplificazione degli adempimenti dei cittadini in materia di Isee e per i relativi controlli sulla veridicità dei dati dichiarati dai beneficiari delle prestazioni sociali agevolate. Al riguardo, l'Autorità ha valutato positivamente il fatto che il Ministero del lavoro e delle politiche sociali si sia adoperato con gli istituti bancari e le Poste italiane s.p.a. per rendere più agevole e non oneroso agli interessati il reperimento del valore della giacenza media da parte degli interessati, rilevante ai fini Isee, e che in tal senso si sono prontamente attivati l'Abi e Poste italiane (parere 7 maggio 2015, n. 265, doc. web n. 4038256).

4.7. *La videosorveglianza in ambito pubblico*

Anche nel 2015, il trattamento di dati personali effettuato tramite sistemi di videosorveglianza in ambito pubblico è stato oggetto di grande interesse.

Settore scolastico

In particolare, in relazione al settore scolastico, l'Ufficio ha avuto occasione di ricordare ad un istituto professionale a seguito di un'istanza di un educatore nonché ad un istituto magistrale, che nel provvedimento generale dell'8 aprile 2010 è stata ribadita la necessità di garantire il diritto dello studente alla riservatezza (art. 2, comma 2, d.P.R. n. 249/1998), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo della personalità dei minori in relazione alla loro vita ed al loro diritto all'educazione. È stato, altresì, evidenziato che può risultare ammissibile l'utilizzo di sistemi di videosorveglianza in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate, attivando gli impianti negli orari di chiusura degli istituti e vietando la messa in funzione delle telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola (punto 4.3, provv. 8 aprile 2010, doc. web n. 1712680).

È stato inoltre chiarito che, laddove la ripresa delle immagini riguardi anche le aree perimetrali esterne degli edifici scolastici, l'angolo visuale deve essere delimitato alle sole parti interessate, escludendo dalle riprese le aree non strettamente pertinenti l'edificio, evidenziando espressamente che il mancato rispetto di quanto prescritto al riguardo comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice (note 15 gennaio e 3 dicembre 2015).

Settore sanitario

Numerosi sono stati i riscontri forniti in relazione a sistemi di videosorveglianza installati in ambito sanitario: in particolare, ad un'Asl, è stato ricordato che nel citato provvedimento generale del 2010 l'Autorità ha evidenziato che l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti, stante la natura sensibile di molti dati che possono essere raccolti, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati. Nel medesimo provvedimento il Garante, nel far presente che devono essere adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e

della dignità delle persone malate, anche in attuazione di quanto prescritto dal provvedimento generale del 9 novembre 2005 (doc. web n. 1191411), ha, altresì, evidenziato che il titolare del trattamento deve garantire che possano accedere alle immagini rilevate per le predette finalità solo i soggetti specificamente autorizzati (ad es., personale medico ed infermieristico) e che devono essere invece previsti, nel caso di reparti dove non sia consentito l'accesso (ad es., rianimazione), adeguati accorgimenti tecnici per limitare la visione dell'immagine, da parte di terzi legittimati (familiari, parenti, conoscenti di ricoverati), solo del proprio congiunto o conoscente. Considerato che le immagini idonee a rivelare lo stato di salute non devono essere diffuse (art. 22, comma 8, del Codice), va evitato il rischio di diffusione delle immagini di persone malate su *monitor* collocati in locali liberamente accessibili al pubblico; al riguardo, è stato rappresentato che il mancato rispetto delle citate prescrizioni comporta l'applicazione della sanzione amministrativa stabilita dall'art. 162, comma 2-*ter*, del Codice (cfr. punto 4.2. del predetto provv. generale). Nella medesima occasione è stata richiamata l'attenzione sulla necessità che il titolare o il responsabile designino per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini (art. 30 del Codice); deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (ad es., registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.) (cfr. punto 3.3.2. del cit. provv.).

È stato chiarito, comunque, che non è riconducibile alla protezione dei dati personali né ai compiti demandati all'Autorità la questione relativa alla necessità o meno che i soggetti che gestiscono l'attività di videosorveglianza rivestano la qualifica di guardia giurata. In ogni caso, ove l'Asl intenda avvalersi del contributo di altri soggetti, per lo svolgimento dei propri compiti istituzionali vanno, comunque, osservate le regole ordinarie in merito alla designazione dei responsabili del trattamento (art. 29 del Codice) (nota 17 marzo 2015).

Nel medesimo settore, l'Ufficio ha fornito alcune precisazioni telative ai casi in cui è necessaria la verifica preliminare del Garante: in particolare, un istituto aveva sotroposto a verifica preliminare la possibilità di installare sistemi di videosorveglianza per la tutela dell'incolumità dei lavoratori, per il controllo delle stanze di degenza e per il monitoraggio dei pazienti ricoverati non autosufficienti e portatori di handicap psichico/fisico; ciò, anche al fine di acquisire ogni informazione necessaria in caso di eventi problematici connessi con la gestione dei pazienti o di eventi delittuosi, considerato che il medesimo istituto era stato in passato coinvolto in una indagine di polizia per malttattamenti degli ospiti della struttura da parte di medici e operatoti sanitari. Al riguardo, l'Ufficio nel ricordare le ipotesi in cui i trattamenti di dati personali effettuati tramite videosorveglianza devono essere sottoposti alla verifica preliminare dell'Autorità, ha fatto presente che i ttattamenti prospettati non fossero riconducibili alle predette ipotesi e, pertanto, non occorreva sottopotli alla vetifica preliminate dell'Autorità. In ogni caso, è stato evidenziato che il sistema di videosorveglianza che si intendeva installare sembrava finalizzato non tanto alla tutela dei lavoratori e pazienti, quanto piuttosto alla prevenzione e repressione dei reati, il cui perseguimento compete alle Forze di polizia; è stata, altresì, rammentata la vigente disciplina di settore sull'attività di controllo a distanza dell'attività dei

lavoratori (nota 8 giugno 2015).

Analogamente, ad una cooperativa che aveva formulato una istanza di verifica preliminare per prolungare sino a tre mesi i tempi di conservazione delle immagini registrate dall'impianto di videosorveglianza, con la finalità di tutela dei beni e della salute degli assistititi in relazione a possibili atti di autolesionismo e di aggressione da parte di altri assistititi e conseguente accertamento di responsabilità civili e penali, è stato rappresentato che, poiché compete esclusivamente alle Forze di polizia il perseguimento di finalità di prevenzione e repressione dei reati e di tutela dell'ordine e della sicurezza pubblica, l'istante non poteva installare sistemi di videosorveglianza per il perseguimento di tali finalità (nota 18 dicembre 2015).

Settore trasporto pubblico

Sempre in relazione ad una richiesta di verifica preliminare, l'Ufficio ha risposto ad una istanza di una azienda di trasporti pubblici che intendeva fornire a coloro che verificano i titoli di viaggio, fotocamere o *smartphone* con lo scopo di consentire l'acquisizione delle immagini degli utenti che, trovati sprovvisti di idoneo titolo di viaggio, al momento della verbalizzazione, non avevano fornito spontaneamente un documento di riconoscimento; ciò, al fine di consentire all'azienda di trasporti di contrastare l'evasione tariffaria, garantire la prevenzione e la repressione dei reati ai danni dell'azienda e dei cittadini, aumentando il senso di sicurezza percepita dall'utenza. Al riguardo, nel far presente che la procedura di identificazione prospettata non risultava conforme alle specifiche disposizioni di settore che già compiutamente disciplinano i presupposti e le modalità di identificazione personale (cfr. art. 11, d.l. 21 marzo 1978, n. 59, convertito con modificazioni, dalla l. 18 maggio 1978, n. 191; artt. 357, 496 e 651 c.p.; artt. 4 e 157, r.d. 18 giugno 1931, n. 773), l'azienda è stata invitata a verificare la conformità dell'iniziativa che si intendeva assumere al quadro normativo sopra richiamato (nota 8 ottobre 2015).

Medesime indicazioni in ordine ai presupposti e alle modalità di identificazione personale sono state fornite ad un'altra azienda provinciale dei trasporti che chiedeva se fosse corretta la procedura in base alla quale i soggetti preposti alla verifica dei titoli di viaggio potessero richiedere, a fini identificativi, il numero di telefono cellulare agli utenti sprovvisti di titolo di viaggio, in caso di impossibilità al riconoscimento degli stessi, per mancata esibizione o possesso del documento di riconoscimento (nota 23 ottobre 2015).

È stato, invece, correttamente sottoposto alla verifica preliminare dell'Autorità un sistema di videosorveglianza intelligente installato da un'autorità portuale presso i porti di sua giurisdizione per le finalità di tutela del patrimonio e delle persone che accedono e lavorano nelle aree portuali. Il sistema prospettato risultava abilitato a svolgere la specifica funzione di attivare un allarme sonoro presso la *control room* in caso di attraversamento di una linea virtuale posta in corrispondenza del limite superiore della recinzione metallica, con lo scopo di segnalare l'eventuale scavalcamento da parte di soggetti non autorizzati della recinzione metallica posizionata lungo il perimetro delle aree ad accesso ristretto (riservate, in taluni porti, a dipendenti, fornitori e passeggeri nelle operazioni di imbarco e sbarco e, in un altro, al personale adibito alle operazioni di movimentazione merci); la citata attività di video analisi è stata ritenuta idonea a rilevare automaticamente, segnalare e registrare un comportamento o evento anomalo, quale può considerarsi l'ingresso in aree qualificate "ad accesso ristretto", in cui la limitazione dell'accesso risultasse adeguatamente segnalata con la presenza di idonei cartelli informativi e con dispositivi di delimitazione delle zone costituiti da barriere *new jersey* sormontate da recinzioni a maglie metalliche. Nello specifico, esaminata la normativa di settore, è stato chiarito che l'autorità portuale, per lo svolgimento delle proprie funzioni istituzionali può legittimamente controllare le aree che rientrano nella sua circoscrizione territo-

riale, con particolare riferimento alle zone ad accesso ristretto, anche attraverso l'installazione di sistemi di videosorveglianza (cfr. att. 6, commi 1, lett. *a*), 2 e 8, l. 28 gennaio 1994, n. 84; art. 1, d.P.R. 29 dicembre 2000; artt. 4, comma 1, lett. *f*); 11, comma 1, lett. *b*) e 18, comma 2, del Codice; regolamento del Parlamento europeo e del Consiglio relativo al miglioramento della sicurezza delle navi e degli impianti portuali n. 725/2004; programma nazionale di sicurezza marittima contro eventuali azioni illecite intenzionali approvato con d.m. del Ministero dei trasporti n. 83/T del 2007). Le caratteristiche specifiche del sistema previsto, inoltre, avendo come unico effetto rispetto all'attivazione dell'allarme quello di richiamare l'attenzione dell'operatore della *control room* al fine di consentirgli di verificare la fondatezza della segnalazione (eventualmente anche azionando delle telecamere "dome", per seguire manualmente l'intruso fino all'arrivo delle guardie giurate), non comportavano l'attivazione di ulteriori funzionalità, quali, ad esempio, l'analisi audio, la geolocalizzazione o il riconoscimento tramite incrocio con ulteriori specifici dati personali, anche biometrici, o confronto con una campionatura precostituita. È stato, pertanto, ritenuto che il sistema intelligente sottoposto a verifica preliminare non arrecasse, in concreto, un pregiudizio rilevante per gli interessati tale da determinare effetti invasivi sulla loro sfera di autodeterminazione e, conseguentemente, sui loro comportamenti. Il Garante lo ha quindi ritenuto proporzionato e ha accolto la richiesta di verifica preliminare, richiamando l'attenzione sulle prescrizioni relative alle misure di sicurezza, con particolare riferimento alle indicazioni contenute nel citato provvedimento del 2010 (cfr. punto 3.3.1.; artt. 31-36 del Codice e All. B al Codice) (provv. 17 settembre 2015, n. 477, doc. web n. 4361006).

Settore rifiuti

In relazione al trattamento di dati personali effettuato tramite videosorveglianza dai comuni, tra i molteplici riscontri forniti, si segnalano le indicazioni rese ad un Comune abruzzese che aveva formulato un quesito in ordine all'utilizzo di "fototrappole" per monitorare l'abbandono incontrollato di rifiuti nelle zone periferiche del territorio comunale; sul punto, l'Ufficio ha fatto presente che l'utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose e a monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente, qualora non risulti possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi (art. 13, l. 24 novembre 1981, n. 689) (cfr. punto 5.2., provv. 8 aprile 2010). Nell'ambito degli specifici adempimenti previsti, è stata richiamata l'attenzione sulle indicazioni fornite dall'Autorità in materia di informativa agli interessati in relazione alla quale il Garante ha messo a disposizione modelli semplificati (cfr. punto 3.1. del predetto provv.; art. 13 del Codice) (nota 4 dicembre 2015).

Ad un Comune campano e ad alcuni segnalanti che lamentavano una presunta violazione della normativa in materia di protezione di dati personali derivante dalle modalità di informazione in ordine alla presenza di sistemi di rilevazione automatica degli accessi in una ztl, così come evidenziato nel citato provvedimento del 2010, è stato rappresentato che, nei casi in cui la normativa di settore preveda espressamente l'obbligo di rendere nota agli utenti l'installazione degli impianti elettronici di rilevamento automatizzato delle infrazioni, è possibile fare a meno di fornire un'ulteriore, distinta informativa rispetto al trattamento dei dati che riproduca gli elementi che sono già noti agli interessati per effetto degli avvisi di cui alla disciplina di settore in tema di circolazione stradale (art. 13, comma 2, del Codice). L'installazione degli avvisi previsti dal codice della strada permette già agli interessati di percepire vari elementi essenziali in ordine al trattamento dei propri dati per-

sonali e idonei pertanto ad adempiere all'obbligo di fornire l'informativa di cui all'art. 13 del Codice (punto 5.3.2. del predetto provv. generale) (note 22 settembre e 1° ottobre 2015).

4.8. *I trattamenti effettuati presso regioni ed enti locali*

Raccolta differenziata dei rifiuti solidi urbani

Nel 2015 l'Autorità si è nuovamente occupata, a seguito di istanze di cittadini e di associazioni di consumatori, della tematica relativa al trattamento dei dati personali effettuato nell'ambito delle modalità di controllo delle procedure di raccolta differenziata dei rifiuti urbani prescelte dai comuni.

In particolare, la questione che ha maggiormente richiesto l'intervento dell'Ufficio ha riguardato l'utilizzo di sacchetti trasparenti per la raccolta differenziata cd. porta a porta, rispetto alla quale, come già negli anni passati, è stata richiamata l'attenzione dei comuni interessati sulla prescrizione contenuta nel provvedimento generale 14 luglio 2005 (doc. web n. 1149822) che considera, in termini generali, non proporzionato l'obbligo di utilizzare un sacchetto trasparente in quanto chiunque si trovi a transitare sul pianerottolo o nell'area antistante l'abitazione può visionare agevolmente il contenuto del sacchetto (cfr. punto 4.a del predetto provv.). In un caso è stato precisato in particolare che i cittadini sono tenuti a utilizzare un mastello chiuso, all'interno del quale depositare i sacchi del rifiuto indifferenziato e che, per utenze con specifiche necessità (ad es., panui e traverse) è possibile rivolgersi ai servizi sociali, per fruire, in forma anonima, di diverse modalità di conferimento quali ad es., i sacchi opachi di colore azzurro (nota 23 gennaio 2015).

Un altro Comune, intetpellato dall'Ufficio, aveva chiarito che la raccolta cd. porta a porta prevedeva che il sacco contenente il rifiuto fosse insetito in appositi contenitori da aprire al momento del ritiro da parte degli operatori (nota 9 gennaio 2015). Infine, un'altra amministrazione comunale, chiamata in causa da numerosi cittadini, aveva dichiarato che i sacchetti previsti per la raccolta di materiali per adulti incontinenti erano in materiale opacizzato e i sacchi per la raccolta di pannolini erano provvisti di *tag*, senza indicare il nome dell'utente, precisando che, in alcune zone periferiche della città, era stata avviata una sostituzione dei sacchetti con bidoni anonimi di diverso colore a seconda della tipologia di rifiuti raccolta (nota 11 marzo 2015).

In un'altra circostanza, invece, l'intervento dell'Ufficio, ha comportato la necessità da parte del Comune interessato di modificare un'ordinanza sindacale, nel senso di eliminare l'obbligo di utilizzare i sacchi trasparenti, consentendo così ai cittadini di conferire i rifiuti in modo che non sia conoscibile il contenuto del sacchetto dall'esterno (nota 21 settembre 2015).

L'istanza di un cittadino ha riguardato un altro aspetto della procedura per la raccolta dei rifiuti ovvero la richiesta, nei confronti dei soggetti conferenti, di esibire un documento di identità al personale preposto alla gestione di apposite aree per il conferimento organizzato dei materiali della raccolta differenziata (cd. piattaforme ecologiche o ecopiazzole), e l'annotazione in un apposito regisrro di nome e indirizzo dei conferenti, della quantità approssimativa del sacchetto nonché del tipo di materiale ricevuto. Al riguardo, è stato rappresentato che alcuni regolamenti comunali prevedono che, nei limiti di una quantità massima giornaliera indicata nel regolamento stesso, in relazione alle diverse tipologie di materiali, i rifiuti siano conferiti senza oneri da parte dei produttori. Nel caso in cui siano superate le quantità indicate per ogni tipologia di rifiuto, il produttore ricorre alla raccolta a domicilio, contattando la società di gestione del servizio, previo pagamento delle spese. In rela-

zione a tale aspetto, deve ritenersi lecito, nei limiti delle finalità istituzionali e ove sia previsto da una disposizione regolamentare (cfr. art. 21, d.lgs. n. 22/1997 ora art. 198, d.lgs. 3 aprile 2006, n. 152), il trattamento dei dati personali (ad es., nome e indirizzo dei conferenti), per la sola finalità di accertamento dell'effettiva residenza nel comune del conferente e per evitare che lo stesso soggetto possa conferire i rifiuti in violazione dei limiti quantitativi ammessi senza oneri a carico dei produttori. Deve essere comunque predisposta un'informativa contenente gli elementi indicati nell'art. 13 del Codice e i dati personali acquisiti devono essere conservati per il solo periodo necessario allo scopo per i quali essi sono stati raccolti (art. 11, comma 1, lett. *d*), (cfr. punto 4.e del predetto provv. generale) (nota 31 dicembre 2015).

Sono state, infine, fornite indicazioni ad un Comune in ordine alla possibilità che ispettori ambientali possano esaminate il contenuto dei sacchetti dei rifiuti, al fine di identificare, attraverso il materiale ispezionato, i presunti trasgressori delle prescrizioni relative alla raccolta differenziata dei rifiuti urbani. In tale circostanza l'Ufficio ha ricordato che agli organi addetti al controllo è riconosciuta la possibilità di procedere a ispezioni di cose e luoghi diversi dalla privata dimora per accertare le violazioni di rispettiva competenza (art. 13, l. 24 novembre 1981, n. 689), ma tale facoltà deve essere esercitata selettivamente, nei soli casi in cui il soggetto che abbia conferito i rifiuti con modalità difformi da quelle consentite non sia in altro modo identificabile. Risulterebbe, quindi, invasiva la pratica di ispezioni generalizzate da parte del personale incaricato (agenti di polizia municipale; dipendenti di aziende municipalizzate) del contenuto dei sacchetti al fine di trovare elementi informativi in grado di identificare, presuntivamente, il conferente (cfr. punto 4.d del predetto provv. generale) (nota 10 settembre 2015).

Dati sensibili

Un Comune ha interpellato il Garante in merito alla sottoscrizione di un protocollo d'intesa con un consolato a sostegno delle famiglie e dei minori, in base al quale il Comune si sarebbe impegnato ad informate il consolato sui casi di affidamento di minori, sui provvedimenti adottati dall'autorità giudiziaria in merito a minori allontanati dalla famiglia, nonché adoperato, unitamente al consolato, affinché l'Ambasciatore venisse nominato curatore speciale del minore. Al riguardo, è stato precisato che in base al Codice, la comunicazione preventiva all'Autorità, ai sensi degli artt. 19, comma 2 e 39, comma 1, può essere effettuata solo qualora ricorrano i presupposti concernenti la natura pubblicistica del soggetto destinatario della comunicazione e la tipologia dei dati, diversi da quelli sensibili e giudiziari. Pertanto, nel caso di specie, trattandosi verosimilmente di comunicazione avente ad oggetto dati sensibili e giudiziari, è srato rappresentato che occorre fare riferimento agli artt. 20 e 22 del Codice, nonché al regolamento sul trattamento dei dati sensibili e giudiziari adottato dal Comune (nota 20 luglio 2015).

L'Autorità si è altresì occupata del trattamento, effettuato dal Consiglio regionale della Toscana, dei dati relativi ad erogazioni liberali effettuate volontariamente dai consiglieri regionali a favore di partiti politici. Al riguardo, il Consiglio regionale ha evidenziato di aver ricevuto la richiesta di effettuare una trattenuta volontaria mensile dal cedolino dello stipendio dei consiglieri e di provvedere ad effettuare l'erogazione liberale ai partiti politici indicati dai richiedenti. L'Ufficio ha chiariro che per il trattamento dei dati relativi alle disposizioni di liberalità a favore di partiti politici, trovano applicazione le regole e le garanzie previste per i dati sensibili, in base alle quali il trattamento è ammesso soltanto in base ad "un'espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite" (artt. 4, comma 1, lett. *d*), 20, 22, del Codice). L'attività sopra descritta, è stata nel frattempo disciplinata dalla l.r. n. 69, 23 ottobre 2015, "Assicurazione pre-

videnziale integrativa e atti di liberalità da attivare su richiesta dei consiglieri e degli assessori regionali. Modifiche alla l.r. 3/2009", che ha previsto che "il consigliere o l'assessore regionale che intenda compiere atti di liberalità, ad esclusione delle donazioni, a favore di soggetti terzi o al fine di acquisire servizi connessi all'esercizio del mandato, può chiedere alla competente struttura del Consiglio regionale di fare da tramite per l'effettuazione della relativa trattenuta e del versamento". Pertanto, in virtù della modifica normativa intervenuta, l'Ufficio ha ritenuto lecita l'attività in parola, qualora effettuata, in conformità alla menzionata normativa, mediante il trattamento delle sole informazioni e delle operazioni strettamente indispensabili previste dal regolamento sul trattamento dei dati sensibili e giudiziari del Consiglio regionale della Toscana, n. 24, 12 febbraio 2014 (scheda n. 4) (nota 10 novembre 2015).

L'Autorità è stata consultata dalla presidenza della Regione Abruzzo in relazione ai trattamenti di dati sensibili connessi all'istituzione di un ufficio di ascolto sociale presso la Regione, al quale cittadini, ma anche gruppi ed associazioni, possono rivolgersi per rappresentare "situazioni personali bisognevoli di attenzioni solidali", al fine di ricercare "iniziative sostenibili per una molteplicità di problematiche scaturenti da difficoltà di carattere sociale" e seguire l'*iter* amministrativo delle vicende prospettate. L'Ufficio ha ritenuto che il regolamento sul trattamento dei dati sensibili e giudiziari della Regione in conformità allo schema tipo, disciplina espressamente i trattamenti dei dati connessi allo svolgimento delle funzioni dell'istituendo ufficio di ascolto sociale (cfr. in particolare la scheda n. 11 allegata al regolamento) (nota 4 marzo 2015).

4.9. *La previdenza e l'assistenza sociale*

Un'associazione Onlus si è rivolta al Garante per una valutazione in merito alla legittimità della richiesta, proveniente dall'Associazione Banco Alimentare del Lazio Onlus (ente capofila), di ottenere la comunicazione delle liste nominative dei propri assistiti e di mettere a disposizione i relativi fascicoli personali, al fine di essere convenzionati con la predetta Associazione capofila e ricevere, per il suo tramite, le risorse alimentari dell'Agenzia per le erogazioni in agricoltura (Agea) da distribuire ai propri assistiti.

L'istruttoria svolta ha evidenziato che l'Agea è l'Organismo intermedio di gestione per l'attuazione del "Programma Operativo sugli aiuti alimentari e l'assistenza materiale" (PO1), per la gestione del quale vengono attinte somme provenienti dal "Fondo di Aiuti Europei agli Indigenti" (FEAD), ai sensi del regolamento (UE) n. 223/2014 del Parlamento Europeo e del Consiglio. Con le "Istruzioni operative n. 22" del 28.8.2014, l'Agea ha fissato le modalità di adesione al programma, in base alle quali le strutture territoriali, ai fini della presentazione della domanda di affiliazione, hanno l'obbligo di tenere un elenco cartaceo o informatico delle persone e dei nuclei familiari assistiti in maniera continuativa e di costituire, per ogni persona o nucleo familiare, un fascicolo che contenga documentazione anagrafica e sullo stato di indigenza (ad es., Isee, affidamento ai servizi sociali, disoccupazione, etc). È inoltre prevista la comunicazione dei dati relativi agli "assistiti continuativi", cioè degli indigenti "per i quali è stata effettuata una valutazione della condizione economica e sociale", nonché degli "assistiti saltuari", cioè di coloro che "vengono assistiti per far fronte a delle emergenze e per i quali l'erogazione avviene senza necessità di verificare la condizione individuale in maniera approfondita", la cui consistenza è stabilita in rapporto al numero totale

degli indigenti continuativi. Pertanto, il trattamento di dati personali dei beneficiari finali è previsto soltanto per gli "assistiti in via continuativa", il cui elenco nominativo deve essere trasmesso all'ente capofila, mentre i fascicoli personali devono essere conservati ed esibiti dalla struttura territoriale solo in fase di convenzionamento o di successive verifiche. Tali controlli, da parte dell'ente capofila, dell'Agea o di suoi delegati, sono previsti dalla normativa comunitaria per verificare la conformità della gestione alle finalità dell'aiuto come stabilito dalle norme del reg. (UE) 223/2014, relativo al Fondo di aiuti europei agli indigenti (v. Titolo V, Gestione e controllo). Con riferimento alla tipologia di dati personali che possono essere trattati dall'Agea, l'Ufficio ha chiarito che la documentazione richiesta agli assistiti continuativi non deve contenere informazioni di natura sensibile, in quanto strettamente finalizzata a comprovare la situazione di disagio economico, come previsto anche dal "Regolamento sul trattamento dei dati sensibili e giudiziari" adottato dall'Agea sul quale il Garante ha espresso il previsto parere (cfr. provv. 18 maggio 2006, doc. web n. 1299152). È stato, inoltre, chiarito che gli enti capofila e gli enti territoriali affiliati, possono trattare i dati personali dei propri aderenti ed assistiti, nel rispetto del quadro normativo di settore, in conformità all'informativa resa agli interessati (artt. 13, 23, 24 e 26 del Codice, autorizzazione generale n. 3 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni, 11 dicembre 2014, n. 585, doc. web n. 3620014) (nota 20 luglio 2015).

Il Garante, con provvedimento 5 febbraio 2015 (n. 62, doc. web n. 3769046), ha espresso parere favorevole sullo schema di decreto direttoriale dell'Inps recante il disciplinare tecnico contenente le regole tecniche di sicurezza per la trasmissione e l'accesso alle informazioni del Sistema informativo Isee-(SII), di cui all'art. 12, comma 2, d.P.C.M. 5 dicembre 2013, n. 159, "Regolamento concernente la revisione delle modalità di determinazione e i campi di applicazione dell'Indicatore della situazione economica equivalente", sul quale il Garante ha fornito il parere di competenza con provvedimento 22 novembre 2012 (n. 361, doc. web n. 2174496). Lo schema di decreto è risultato conforme alle indicazioni fornite dall'Ufficio ai competenti uffici dell'Istituto nel corso di numerosi contatti, anche informali, volti a garantire il rispetto della disciplina in materia di protezione dei dati personali nell'ambito delle operazioni di raccolta e successivi trattamenti dei dati personali effettuati attraverso il SII e necessari al calcolo dell'Isee. Le principali indicazioni hanno riguardato le modalità di trattamento e le misure di sicurezza poste a garanzia dei dati trattati, nell'ambito delle quali è stato previsto, in particolare, che i flussi di dati per l'alimentazione del SII, tramite applicazioni web, avvenga su rete pubblica con l'utilizzo del protocollo SSL per garantire il trasporto cifrato delle informazioni. Nelle ipotesi in cui i flussi di dati vengono effettuati tramite cooperazione applicativa, invece, è stato previsto che si faccia riferimento al modello *advanced* di porta di dominio definito negli *standard* SPC di cooperazione applicativa e che la verifica degli accessi avvenga sulla base della mutua autenticazione fra i *server* dell'Istituto e quelli degli enti coinvolti. Sono stati ribaditi, inoltre, i princìpi di pertinenza, non eccedenza ed indispensabilità dei dati rispetto alle finalità perseguite, anche in riferimento alla consultazione delle informazioni autodichiarate da parte dell'ente erogatore per finalità di controllo e, a garanzia del rispetto di tali princìpi, sono stati previsti specifici controlli a campione da parte dell'Istituto (art. 11, commi 6 e 10, d.P.C.M. 5 dicembre 2013, n. 159; art. 11, comma 2, del Codice). Sono state individuate specifiche tecniche di anonimizzazione e aggregazione dei dati ai quali gli enti erogatori possono accedere a fini di programmazione dei singoli interventi nonché dei dari che devono essere trasmessi

al Ministero del lavoro e delle politiche sociali e, in caso di specifica richiesta, alle regioni e alle province autonome, per effettuare elaborazioni a fini di programmazione, di ricerca e di studio (art. 11, commi 4, 10, e 12, d.P.C.M. 5 dicembre 2013, n. 159). Particolare attenzione è stata posta sulle modalità di realizzazione dei controlli che la Guardia di finanza effettua sulla posizione reddituale e patrimoniale dei nuclei familiari dei soggetti beneficiari di prestazioni (art. 11, commi 11 e 13, d.P.C.M. 5 dicembre 2013, n. 159; 4, comma 2, d.m. 8 marzo 2013). Al riguardo, lo schema di decreto direttoriale esaminato evidenzia che gli accessi della Guardia di finanza avvengono in modalità web ovvero tramite cooperazione applicativa. Dal punto di vista funzionale, tali accessi si differenziano in due categorie: quelli effettuati nell'ambito di indagini specifiche e quelli effettuali nell'ambito della programmazione dell'attività di accertamento. Nel primo caso la Guardia di finanza può avere accesso all'attestazione riportante l'Isee, al contenuto della dsu, nonché agli elementi informativi necessari al calcolo, acquisiti dagli archivi amministrativi dell'Inps e dell'Agenzia delle entrate; nel secondo, il controllo della posizione reddituale e patrimoniale dei nuclei familiari dei soggetti beneficiari di prestazioni deve avvenire secondo criteri selettivi da definire, previo parere del Garante, in attuazione del protocollo di intesa adottato al fine di disciplinare le regole generali della reciproca collaborazione tra Inps e Guardia di finanza. L'Inps ha previsto che i caf e i comuni possano ricevere per gli interessati l'attestazione Isee, le dsu nonché gli elementi informativi necessari al calcolo dell'Isee. A tal fine, come indicato in fase istruttoria, i predetti soggetti devono inviare all'Istituto medesimo copia del mandato di assistenza, corredato dal documento di riconoscimento dell'interessato.

Al fine di impedire la creazione di autonome banche dati delle dsu presso i soggetti legittimati alla ricezione della stessa, l'Istituto ha predisposto una specifica funzione di *audit* e notifica sulla frequenza e numerosità delle posizioni interrogate nonché la registrazione dell'identificativo dell'operatore dell'ente che effettua l'accesso e del codice della posizione acceduta (artt. 10, comma 6, e 11, comma 4, d.P.C.M. 5 dicembre 2013, n. 159).

Il Garante, con provvedimento 2 aprile 2015 (n. 195, doc. web n. 3843693), ha espresso parere favorevole sullo schema di decreto direttoriale dell'Inps inerente le modalità attuative dei flussi informativi e disciplinare tecnico per la sicurezza della banca dati delle prestazioni sociali agevolate istituita presso l'Inps con decreto interministeriale dell'8 marzo 2013 al fine di rafforzare i controlli connessi all'erogazione di prestazioni sociali agevolate condizionate all'Isee (sul quale il Garante aveva fornito il parere di competenza con provv. 17 gennaio 2013, n. 14, doc. web n. 2300596) (artt. 2, comma 5, e 5 comma 5, d.m. 8 marzo 2013). La predetta banca dati è alimentata dagli enti locali e da ogni altro ente erogatore di prestazioni sociali agevolate, con le informazioni sulle prestazioni sociali agevolate, condizionate all'Isee, e sui soggetti che ne hanno beneficiato (art. 2, commi 1, 2 e 3, d.m. 8 marzo 2013). Ad essa accedono l'Inps, l'Agenzia delle entrate e la Guardia di finanza per lo svolgimento di attività di controllo (art. 4, commi 1 e 2, d.m. cit.). Le informazioni contenute nella banca dati sono poi trasmesse a diversi soggetti pubblici in forma anonima e aggregata per finalità di programmazione e monitoraggio nonché per elaborazioni a fini statistici, di ricerca e di studio (art. 4, commi 4, 5 e 6). Sulla base delle indicazioni fornite dall'Ufficio, l'Inps ha, in primo luogo, previsto che le convenzioni bilaterali per la definizione delle modalità tecniche e delle misure di sicurezza per l'accesso ai dati della banca dati prestazioni sociali agevolate da parte dell'Agenzia delle entrate e della Guardia di finanza debbano essere preventivamente sottoposte al Garante per le valutazioni di competenza. In secondo luogo, partico-

lare attenzione è stata posta alle tecniche di anonimizzazione ed alle modalità di aggregazione dei dati personali contenuti nella banca dati che l'Inps deve fornire a Ministero del lavoro e delle politiche sociali, regioni e province autonome, comuni e altri enti pubblici responsabili della programmazione di prestazioni e di servizi sociali e socio-sanitari ed al Mef-Dipartimento della Ragioneria (art. 4, commi 4, 5 e 6). In particolare, sono state individuati specifici livelli di aggregazione (su base territoriale) e cadenze temporali (annuale) per la comunicazione dei dati al Mef per finalità di monitoraggio con l'adozione di ogni opportuna cautela al fine di impedire l'identificazione di singoli interessati. È stata, inoltre, puntualmente descritta la tecnica di anonimizzazione dei dati che l'Inps deve fornire al Ministrero del lavoro e delle politiche sociali, regioni, province autonome, comuni e altri enti pubblici responsabili della programmazione di prestazioni e di servizi sociali e socio-sanitari per finalità di monitoraggio, programmazione nonché per elaborazioni a fini statistici, di ricerca e di studio. Tale procedura prevede, in particolare, che a ciascuna posizione venga associato un codice numerico avente natura causale e non progressiva, senza alcun riferimento ai dati oggetto di trattamento, creato appositamente per anonimizzare i dati in questione e non conservato dall'Inps. Anche in questo caso sono stati previsti valori soglia per le variabili di osservazione, in modo da non trasmettere le posizioni per le quali si potrebbe risalire all'individuazione del soggetto ed è stato precisato che l'Inps fornirà le predette informazioni con riferimento ad una finestta temporale non superiore a tte anni, facendo esplicito divieto di diffondere le informazioni ricevute. Gli enti erogatori possono inviare i dati relativi alle prestazioni sociali agevolate o facendo un invio massivo tramite *upload* di un *file* ovvero ttamite acquisizione interattiva attraverso l'inserimento manuale su una web *form*. Al riguardo, con specifico riferimento alla trasmissione dei dati tramite cooperazione applicativa, è stato specificato, coerentemente con le indicazioni emerse nella fase istruttoria, che viene fatto uso di modelli *advanced* di porta di dominio. Le comunicazioni avvengono in modalità *https* e la verifica degli accessi viene basata sulla mutua autenticazione.

È stato previsto, inoltre, che gli accessi ai servizi *online* sono consentiti solo ad operatori espressamente autorizzati da parte dell'ente, dotati di credenziali personali e non cedibili, tramite l'uso di postazioni di lavoro connesse alla rete IP dell'ente. Al riguardo, l'Inps ha imposto agli enti che accedono alla banca dati in parola di individuare ogni misura atta a garantire che l'accesso avvenga da postazioni specificamente autorizzate inoltre ha esplicitamente previsto il ricorso, per l'accesso ai servizi *online*, all'infrastruttura Spid. Al fine di evitate la duplicazione delle informazioni raccolte nella banca dati, sono stati previsti sistemi di tracciamento, *auditing* e notifica attraverso i quali l'Istituto può verificare la frequenza e la numerosità delle posizioni interrogate ed, eventualmente, sospendere l'accesso dell'utenza del soggetto che risulta aver raggiunto determinate soglie di attenzione. L'Inps ha precisato infine che i dati delle prestazioni sociali agevolate verranno conservati per un periodo di cinque anni oltre il quale saranno archiviati e conservati con i sistemi di *back up* dell'Istituto e, salve le ipotesi previste dalle legge, non saranno accessibili da soggetti terzi.

Il Garante ha reso parere favorevole sullo schema di decreto direttoriale dell'Inps recante il disciplinare tecnico conrenente le "Misure di sicurezza per il trattamento dei dati personali di cui al d.m. 10 gennaio 2013 - attuazione della sperimentazione della nuova carta acquisti - modalità di trasmissione dei dati tra l'Inps e i comuni, livelli e modalità di accesso selettivo ai dati, tracciabilità degli accessi e termini di conservazione dei relativi dati" (provv. 12 marzo 2015, n. 143, doc. web n. 3863732) (art. 11, comma 2, d.m. 10 gennaio 2013).

L'art. 60, d.l. 9 febbraio 2012, n. 5, convertito con modificazioni in l. 4 aprile 2012, n. 35 ha previsto che venga avviata una sperimentazione, nei comuni con più di 250.000 abitanti, volta a favorire la diffusione della carta acquisti tra le fasce di popolazione in condizione di maggiore bisogno (art. 81, comma 32, d.l. 25 giugno 2008, n. 112, convertito, con modificazioni, dalla l. 6 agosto 2008, n. 133) ed ha affidato ad un decreto del Ministro del lavoro e delle politiche sociali, adottato di concerto con il Mef, la definizione delle disposizioni per l'attuazione della sperimentazione della nuova carta acquisti (d.m. 10 gennaio 2013, sul quale il Garante ha fornito il proprio parere di competenza in data 6 dicembre 2012, n. 395, doc. web n. 2216848). Il citato decreto prevede che il cd. soggetto attuatore (Inps) adotti un provvedimento concernente le misure di sicurezza per i trattamenti dei dati personali previsti dal decreto, le modalità di trasmissione dei dati tra lo stesso ed i comuni, i livelli e le modalità di accesso selettivo ai dati, la tracciabilità degli accessi e i termini di conservazione dei relativi dati, su conforme parere del Garante, entro tre mesi dall'entrata in vigore del decreto stesso (art. 11, comma 2). Lo schema di decreto presentato è risultato conforme alle numerose indicazione fornite dall'Ufficio ai competenti uffici dell'Istituto nel corso di contatti, anche informali.

4.10. *L'attività giudiziaria*

Sicurezza nelle intercettazioni

Con provvedimento 25 giugno 2015, n. 375 (doc. web n. 4120817) l'Autorità è nuovamente intervenuta sulla delicata materia delle misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica, con riferimento alle prescrizioni oggetto del provvedimenro 18 luglio 2013, n. 356 (doc. web n. 2551507) i cui termini per l'adempimento erano già stati differiti con provvedimento 26 giugno 2014, n. 322 (doc. web n. 3235971).

Al riguardo, sulla base sia della documentazione trasmessa dal Ministero della giustizia sul monitoraggio dello stato di attuazione delle misure, sia degli approfondimenti svolti presso il Ministero da un tavolo di lavoro a carattere interistituzionale, si è riconosciuto il carattere prioritario alle criticità riguardanti le misure informatiche, di più immediato ed incisivo impatto sulla sicurezza dei trattamenti.

Pertanto si è provveduto nuovamente a differire i termini per l'adempimento di alcune misure informatiche, con riserva di valutare successivamente se l'attuazione di tali misure, e delle altre che siano poste in essere, anche alla luce dell'evoluzione tecnologica, consenta di supetare le prescrizioni di tipo strutturale imposte con il provvedimento del 2013, il cui termine di attuazione è stato, pertanto, sospeso.

Pubblicazione di sentenze a fini di informazione giuridica

È pervenuta a questa Autorità una segnalazione con cui si è lamentata la facile reperibilità in internet di un'ordinanza giudiziaria, recante i dati identificativi, dati sensibili e informazioni di natura sanitaria relativi all'interessato. Al riguardo l'Autorità, nel rappresenrare che l'interessato non si era potuto avvalere della facoltà di richiedere l'anonimizzazione dell'ordinanza non essendosi costituito in giudizio (cfr. art. 52, comma 1, del Codice e le Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica adottate il 2 dicembre 2010, doc. web n. 1774813), ha invitato il Tribunale amministrativo che aveva adottato l'ordinanza a valutare l'opporrunità di anonimizzazione disposta d'ufficio oppure, in alrernativa, l'adozione di accorgimenti tecnici idonei ad evitare l'indicizzazione nei motori di ricerca dell'ordinanza pubblicata sul sito isriruzionale (nota 16 marzo 2015). Il Tribunale ha provveduto

ad oscurare il nome dell'interessato.

Anche nel 2015 sono pervenute all'Autorità segnalazioni relative al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata introdotto dalla riforma del processo esecutivo (d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, dalla l. 14 maggio 2005, n. 80), che prevede la pubblicazione in appositi siti internet di copia dell'ordinanza del giudice che dispone sulla vendita forzata e della relazione di stima dei beni da espropriare. Al riguardo, con una segnalazione veniva lamentata la pubblicazione sul sito istituzionale di un Tribunale di avvisi d'asta che recavano, tra le altre informazioni, i nominativi delle parti debitrici. L'Autorità, pur verificando che allo stato attuale gli avvisi non contenevano dati personali relativi agli interessati, ha richiamato l'attenzione del Presidente del Tribunale ove si svolgevano le procedure sulla necessità di applicare la vigente normativa in materia di esecuzioni immobiliari conformemente alla normativa in materia di protezione dei dati personali e alle vigenti prescrizioni di cui agli artt. 174, comma 9, del Codice e 490, comma 3, c.p.c. al fine di assicurare la piena tutela dei diritti dei debitori sottoposti all'esecuzione. L'Autorità ha ricordato, in particolare, di avere già invitato, con provvedimento 7 febbraio 2008 (doc. web n. 1490838) gli uffici giudiziari e i professionisti delegati alle operazioni di vendita nelle esecuzioni immobiliari ad omettere, conformemente a quanto prescritto dagli artt. 174, comma 9, del Codice e 490, comma 3, c.p.c., l'indicazione del debitore e di eventuali terzi estranei alla procedura dagli avvisi d'asta, estendendo tale omissione anche alla documentazione allegata ai predetti avvisi (nota 2 febbraio 2015).

Pubblicità dei dati nei procedimenti di espropriazione forzata

Con riferimento alla produzione documentale in sede giudiziaria, il Garante, nel ricordare preliminarmente che l'art. 24, comma 1, lett. *f*), del Codice consente il trattamento di dati personali senza consenso laddove il trattamento sia indispensabile per far valere o difendere un diritto in sede giudiziaria, ha confermato che spetta al giudice adito, ove ritualmente richiesto, la competenza a valutare la liceità del trattamento dei dati personali. Infatti, l'art. 160, comma 6, del Codice srabilisce che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali, ancorché non conforme a disposizioni di legge o di regolamento, restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (note 10 aprile, 13 e 14 maggio, 1° giugno, 8 luglio, 16 ottobre e 6 novembre 2015). L'art. 160, comma 6, del Codice è stato richiamato dall'Autorità con riferimento ad altre segnalazioni relative a trattamenti di dati personali nel corso di procedimento giudiziario (note 6 e 27 novembre 2015).

Produzione di documenti in giudizio

Con riferimento ad altre segnalazioni con cui si lamentava la notifica di atti giudiziari a soggetti estranei alle relative procedure giudiziarie, il Garante ha fatto presente che, trattandosi di atti inerenti al giudizio civile, la loro valutazione spetta al giudice adito ai sensi dell'art. 160, comma 6, del Codice. In un caso, l'Autorità ha tuttavia rappresentato che, laddove l'interessato ritenga che l'atto giudiziario, in quanto notificato ad estranei, si caratterizzi per il suo contenuto lesivo e si collochi al di fuori di un trattamento per finalità di giustizia, può valutare se sia utilizzabile l'interpello di cui all'art. 8 del Codice per far valere nei confronti del titolare del trattamento il diritto alla cancellazione dei dati trattati in violazione di legge ai sensi dell'art. 7, comma 3 lett. *b*) (nota 27 novembre 2015).

Notificazioni di atti giudiziari a soggetti estranei alle procedure

In un altro caso, invece, essendo stata interessata altresì la Procura della Repubblica, l'Autorità ha affermato che l'impossibilità di interferire con l'attività dell'autorità giudiziaria, dotata di poteri di accertamento ben più penetranti di quelli spettanti al Garante, e la necessità di rispettare i diritti dei soggetti coinvolti (quali, in ipotesi, la facoltà di non rendere dichiarazioni, *ex* art. 64 c.p.p.), rendono,

nei fatti, inattuabili gli accertamenti da parte di questa Autorità, indispensabili per assumere le determinazioni di competenza. Del resto, le verifiche che spettano a questa Autorità possono risultare condizionate anche all'esito dell'esposto, quanto meno in ordine all'accertamento dei fatti. Ove perdurasse l'interesse alle determinazioni dell'Autorità, si è chiesto pertanto all'interessato di dare notizia dell'esito del procedimento civile e della querela dallo stesso presentato, per consentire di valutare se residuino margini per le decisioni di competenza dell'Autorità medesima (nota 21 aprile 2015).

Anche con riferimento ad altre segnalazioni, che sono state oggetto di esposti e querele alla Procura della Repubblica, l'Autorità ha sottolineato, tra l'altro, l'impossibilità di interferite con l'attività dell'autorità giudiziaria (nota 10 aprile, 1° giugno, 16 ottobre e 6 novembre 2015).

Acquisizione del certificato penale e comunicazioni di dati giudiziari

A seguito di una segnalazione, l'Autorità si è occupata di alcuni trattamenti di dati giudiziari effettuati da un Tribunale in modo non conforme a quanto sancito dal Codice. In particolare, è stato rilevato che l'acquisizione del certificato penale relativo al segnalante da parte del Tribunale, presso il quale il medesimo segnalante rivestiva il ruolo di assistente amministrativo, sarebbe avvenuta impropriamente "per ragioni di giustizia" *ex* art. 21, d.P.R. 313/2002, mentre appariva correttamenre riferibile alla previsione di cui all'art. 28, d.P.R. 313/2002. Si accertava, altresì, l'avvenuta comunicazione, non in conformità al Codice, dei dati giudiziari relativi al segnalante da parte del Tribunale alla Procura della Repubblica, nonché al Consiglio della magistratura militare. Ciò in quanto il trattamento di dati giudiziati da parte di soggetti pubblici deve essere autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (art. 21 del Codice), che invece nel caso di specie mancavano. Ciò considerato non si sono, tuttavia, ravvisati gli estremi per l'adozione di un provvedimento da parte dell'Autorità, avendo tali condotte esaurito i loro effetti, restando comunque salva la facoltà per l'interessato di adire l'autorità giudiziaria ordinaria per il risarcimento di eventuali danni subiti (nota 25 agosto 2015).

5 La sanità

5.1. *I trattamenti per fini di cura*

Continuano a pervenire numerose segnalazioni in merito al mancato rispetto delle disposizioni in materia di tutela dei dati personali da parte di strutture sanitarie pubbliche e private nell'erogazione dei servizi di diagnosi, cura e riabilitazione degli assistiti.

A seguito della segnalazione di un cittadino, l'Ufficio ha verificato che sul sito web di un'Asl era possibile consultare i dati anagrafici degli assistiti che si erano registrati sullo stesso per usufruire dei servizi *online*. In particolare, inserendo parte di un nome o di un cognome, si potevano consultare le relative schede anagrafiche nelle quali erano riportati la residenza, il codice fiscale e il numero di telefono degli assistiti ed era, inoltre, possibile modificare tali dati nonché cancellare l'*account*. Il Garante ha, così, vietato la diffusione dei dati personali degli assistiti registrati sul portale dell'azienda, rilevando l'illiceità del trattamento effettuato e ha ricordato alle pp.aa. che offrono servizi in rete di adottare idonee misure di sicurezza tali da ridurre al minimo i rischi di accesso non autorizzato o di trattamenti di dati non consentiti (provv. 17 dicembre 2015, n. 665, doc. web n. 4630534). Sebbene l'azienda abbia prontamente adempiuto, bloccando l'accesso indiscriminato ai dati, l'Autorità si è, comunque, riservata di approfondire il caso e ha al contempo avviato un autonomo procedimento sanzionatorio per le violazioni riscontrate.

In altri casi l'Ufficio è intervenuto in relazione ad iniziative promosse dalle aziende sanitarie che prevedevano il trattamento dei dati sulla salute degli assistiti. In un caso, due aziende sanitarie avevano manifestato l'intenzione di implementare un nuovo servizio consistente nel rendere automaticamente disponibili agli organi di stampa le informazioni sugli interventi effettuati dalla Centrale operativa 118 attraverso un collegamento telematico con i sistemi informativi aziendali. Al riguardo, l'Ufficio ha evidenziato i significativi profili di criticità connessi all'automatica messa a disposizione degli organi di stampa dei dati sanitari rilevati negli interventi in emergenza di tutti i pazienti a prescindere dalla rilevanza pubblica della notizia. A seguito dell'intervento dell'Ufficio le aziende sanitarie hanno modificato il progetto non consentendo il collegamento telematico tra gli applicativi in uso presso i servizi del 118 e gli organi di stampa (nota 20 aprile 2015).

Ulteriori chiarimenti sono stati resi nei confronti dei medici di medicina generale con riferimento alle cautele da adottare nella consegna delle ricette o di altri certificati medici qualora – su richiesta dell'interessato – la suddetta documentazione non sia consegnata direttamente ma, ad esempio, da un farmacista indicato dallo stesso interessato. In tali casi è indispensabile che il documento sia contenuto all'interno di una busta chiusa. Qualora l'interessato intenda far ritirare la suddetta documentazione da parte di un terzo (ad es., un parente o un convivente) è necessario che quest'ultimo, al momento del ritiro, esibisca una delega scritta (nota 23 febbraio 2015).

L'Ufficio è intervenuto in merito all'abbandono di documentazione clinica presso locali in disuso di strutture sanitarie dando avvio a un procedimento sanzionatorio per mancata adozione delle misure di sicurezza (nota 5 novembre 2015).

5.1.1. L'informativa e il consenso al trattamento dei dati sanitari

Sono pervenute numerose segnalazioni nelle quali i pazienti lamentano di non aver manifestato il proprio consenso al trattamento dei dati sanitari e di non aver ricevuto alcuna informativa in merito all'utilizzo degli stessi o di aver ricevuto al riguardo informazioni insufficienti o lacunose. Le maggiori criticità riscontrate nelle istruttorie hanno riguardato modelli di informativa e consenso nei quali non venivano evidenziati i trattamenti di dati indispensabili all'erogazione della prestazione medica rispetto a quelli facoltativi (ad es., per finalità di ricerca scientifica, offerta di altri servizi, campagne di prevenzione). L'omissione di tale specificazione non consentiva al paziente di comprendere le conseguenze del mancato conferimento del consenso con specifico riferimento alla possibilità di usufruire della prestazione medica richiesta.

A seguito degli interventi dell'Ufficio numerose strutture sanitarie hanno modificato i propri modelli di informativa e di consenso. L'Autorità ha, tuttavia, avviato un procedimento sanzionatorio nei confronti delle predette strutture (note 23 febbraio e 20 maggio 2015).

In relazione all'incremento dei servizi riconducibili alla sanità digitale e alla necessità di regolamentare tale settore, il Garante ha accolto l'invito del Ministero della salute partecipando, già dal mese di luglio, al tavolo di lavoro interistituzionale sulla *m-Health* e sulle *apps* in ambito medico cui partecipa, tra gli altri, il Ministero dello sviluppo economico, l'Istituto superiore di sanità, l'AgID, l'Aifa e l'Università Tor Vergata. Particolare attenzione sarà data all'aspetto dell'informativa e all'acquisizione del relativo consenso.

5.1.2. Il Fascicolo sanitario elettronico e i dossier *sanitari*

Nel periodo di riferimento è stato adottato il primo dei decreti attuativi del Fascicolo sanitario elettronico (di seguito Fse). Con il d.P.C.M. 29 settembre 2015, n. 178 sono stati, infatti, definiti i contenuti del Fse, le responsabilità e i compiti dei soggetti coinvolti, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali, le modalità e i livelli diversificati di accesso in relazione alle specifiche finalità, i criteri di interoperabilità, nonché i contenuti informativi e le codifiche del profilo sanitario sintetico e del referto di laboratorio, individuati quali primi contenuti da attivare a livello nazionale.

Su tale decreto l'Autorità aveva espresso parere favorevole nel 2014 (n. 261, doc. web n. 3230826). Lo schema di decreto, elaborato nell'ambito di un tavolo di lavoro istituito presso il Ministero della salute cui ha partecipato l'Ufficio fin dalla sua costituzione nel gennaio 2013, prevede, in particolare, che il paziente sia informato chiaramente e possa decidere con consapevolezza se dare il consenso all'alimentazione del Fse, e in caso positivo, decidere se dare anche il consenso per finalità di cura (in mancanza del quale il fascicolo potrà essere utilizzato solo per finalità di monitoraggio, programmazione e ricerca, con le dovute garanzie di anonimato).

Con riferimento ai trattamenti di dati personali effettuati attraverso il *dossier* sanitario, l'Autorità ha inteso diramare le Linee guida in materia di *dossier* sanitario, al fine di definire un quadro di riferimento unitario per il corretto trattamento dei dati raccolti nei *dossier*, già istituiti o che si intendono istituire, da parte di strutture sanitarie pubbliche e private (provv. 4 giugno 2015, n. 331, doc. web n. 4084632).

Le numerose istruttorie poste in essere negli anni precedenti avevano fatto emergere la necessità di fornire alcuni chiarimenti soprattutto in merito ai principali adempimenti previsti. Affinché i *dossier* sanitari utilizzati presso le strutture sanitarie rappresentino uno strumento di ausilio nei processi di diagnosi e cura dei pazienti, è necessario che gli stessi siano realizzati in maniera da garantire la certezza

dell'origine, la correttezza dei dati e l'accessibilità degli stessi solo da parte di soggetti legittimati. Il provvedimento del Garante stabilisce, in particolare, che ai pazienti deve essere consentito di scegliere, in piena libertà, se far costituire o meno il *dossier* sanitario. In assenza del consenso il medico avrà a disposizione solo le informazioni rese in quel momento dal paziente o in precedenti prestazioni fornite dallo stesso professionista. La mancanza del consenso non deve incidere minimamente sulla possibilità di accedere alle cure mediche richieste. Per poter inserire nel *dossier* informazioni particolarmente delicate (infezioni HIV, interventi di interruzione volontaria della gravidanza, dati relativi ad atti di violenza sessuale o pedofilia) sarà necessario un consenso specifico.

Per consentire al paziente di scegliere in maniera libera e consapevole, la struttura dovrà informarlo in modo chiaro, indicando in particolare, chi avrà accesso ai suoi dati e che tipo di operazioni potrà compiere. Ne deriva, quindi, che nell'informativa al *dossier* deve essere sottolineata l'intenzione da parte del titolare del trattamento di costituire un insieme di informazioni riguardanti l'interessato quanto più complete, che possano documentare parte della sua storia sanitaria attraverso un sistema integrato da parte del personale sanitario che lo avrà in cura; allo stesso tempo l'interessato deve essere informato che, in caso di mancato consenso al trattamento dei dati personali mediante *dossier*, non vedrà preclusa la possibilità di accesso alle cure richieste.

La struttura sanitaria inoltre, dovrà garantire al paziente l'esercizio dei diritti riconosciuti dal Codice (accesso ai dati, integrazione, rettifica, etc.) e la conoscenza del reparto, della data e dell'orario in cui è avvenuta la consultazione del suo *dossier*. Molte delle segnalazioni pervenute al Garante lamentavano accessi al *dossier* sanitario avvenuti per scopi personali (curiosità, cause giudiziarie tra le parti, etc.) o per fini commerciali da parte di personale amministrativo o di personale sanitario che non era mai stato coinvolto nel processo di cura dell'interessato. Tali casi hanno messo in risalto i rischi di accesso non autorizzato e hanno portato l'Autorità a prevedere che l'interessato possa chiedere al titolare del trattamento quali siano stati gli accessi al proprio *dossier*, con l'indicazione del reparto/struttura e della data e dell'ora dell'accesso.

Al paziente dovrà essere, inoltre, garantita la possibilità di oscurare alcuni dati o documenti sanitari che non intende far confluire nel *dossier* mediante il sistema dell'"oscuramento dell'oscuramento" ovvero con modalità tali da non rendere palese la menzionata decisione a chi legittimamente accede ai dati.

Considerata la particolare delicatezza del *dossier* il Garante ha prescritto l'adozione di elevate misure di sicurezza. I dati sulla salute dovranno essere separati dagli altri dati personali e dovranno essere individuati criteri per la cifratura dei dati sensibili. L'accesso al *dossier* sarà consentito solo al personale sanitario coinvolto nella cura. Ogni accesso e ogni operazione effettuata, anche la semplice consultazione, saranno tracciati e registrati automaticamente in appositi *file* di *log* che la struttura dovrà conservare per almeno 24 mesi.

Eventuali violazioni di dati o incidenti informatici dovranno essere comunicati all'Autorità, entro quarantotto ore dalla conoscenza del fatto, attraverso un modulo predisposto dal Garante all'indirizzo: databreach.dossier@pec.gpdp.it.

Alla fine del 2015, dopo l'adozione delle suddette Linee guida l'Autorità è intervenuta con riferimento al tratramento dei dati effettuato tramite il *dossier* sanitario da parte di un'Asl (provv. 22 ottobre 2015, n. 550, doc. web n. 4449114).

Le irregolarità emerse nel corso di un accertamento ispettivo riguardavano il modello di informativa e la mancanza del consenso del paziente per la costituzione del *dossier* sanitario. Il sistema informativo aziendale era poi strutturato in modo tale che l'operatore sanitario potesse effettuare ricerche non solo con riferimento ai pro-

pri pazienti, ma anche a soggetti che non aveva in cura ma che avevano sostenuto un esame clinico presso l'azienda.

Ciò premesso il Garante ha prescritto all'Asl di regolare gli accessi al sistema informativo aziendale, rendendo consultabili i documenti sanitari del paziente contenuti nel *dossier* solo da parte del professionista che lo ha in cura, nonché di integrare il modello dell'informativa in uso, specificando, tra l'altro, i diritti dell'interessato e le modalità attraverso le quali è possibile revocare il consenso ed oscurare uno o più eventi clinici.

L'Ufficio ha, inoltre, in corso ulteriori attività istruttorie in merito alla presunta violazione della disciplina il materia di protezione dei dati personali che si sarebbe verificata a seguito di accessi abusivi al *dossier* sanitario di un paziente da parte di professionisti sanitari che non lo avevano in cura. In uno dei casi in esame tale consultazione sarebbe stata possibile simulando un accesso in emergenza del paziente, in altri casi mediante un accesso diretto al *dossier* in quanto il sistema informativo è risultato privo di meccanismi di profilazione degli utenti.

In un altro caso, con riferimento al *dossier* sanitario utilizzato nell'ambito di un sistema informativo integrato tra i vari servizi di neuropsichiatria infantile regionali, l'Ufficio ha riscontrato alcune criticità in merito alle modalità di condivisione dei dati tra i vari servizi, con particolare riferimento alla circostanza che nella maggior parte dei casi il paziente veniva effettivamente seguito da un solo servizio di neuropsichiatria. A seguito dell'intervento dell'Ufficio, il sistema è stato modificato non consentendo più la possibilità di condivisione dei dati clinici dei minori a livello regionale (nota 21 dicembre 2015).

5.1.3. I referti e la documentazione sanitaria

Nel 2015 vi è stato un incremento delle segnalazioni relative alla consegna di documentazione sanitaria a soggetti diversi dall'interessato sprovvisti di delega. In molti dei casi esaminati la consegna di referti, lettere di dimissione ospedaliera o cartelle cliniche è avvenuta per errore umano dettato dal mancato rispetto delle disposizioni dettate dalla struttura sanitaria in occasione del ritiro della documentazione medica.

Le fattispecie esaminate hanno riguardato, in particolare, informazioni sanitarie riferite a soggetti terzi contenute nella documentazione consegnata all'interessato e la consegna di referti a soggetti non muniti di delega.

Nei casi segnalati, nei confronti dei quali è stato aperto un procedimento amministrativo sanzionatorio, le strutture sanitarie interessate hanno intrapreso azioni correttive nel processo di consegna dei referti, migliorando le procedure di archiviazione della documentazione medica e realizzando una maggiore formazione del personale coinvolto (note 15 gennaio, 9 aprile, 28 luglio e 21 dicembre 2015).

Merita particolare attenzione quanto segnalato da un paziente che aveva ricevuto dalla struttura sanitaria presso la quale si era recato per alcune analisi cliniche le credenziali di accesso al servizio di ritiro dei referti *online* relative alla prestazione erogata in favore di un altro paziente (nota 16 dicembre 2015).

Analogamente, l'Autorità è intervenuta in merito alla consegna in busta aperta presso una farmacia comunale dei referti relativi alle analisi di laboratorio eseguiti presso un'Asl locale. Anche in tal caso, dopo l'intervento dell'Ufficio, sono state predisposte azioni migliorative nonché calendarizzata un'attività formativa nei confronti di tutto il personale dei vari *front office* (nota 4 settembre 2015).

Richieste su delega dell'autorità giudiziaria

Una unità sanitaria locale ha posto al Garante un quesito sulla condotta da assumere a fronte delle richieste di fornire documentazione relativa ad un paziente della struttura, da parte della polizia giudiziaria su delega dell'autorità giudiziaria, Il Garante, considerato che la menzionata attività risulta ricompresa nella previsione

dell'art. 47 del Codice secondo cui, in caso di trattamento di dati personali effettuato – per ragioni di giustizia – presso uffici giudiziari alcune disposizioni del Codice non si applicano, ha rilevato che la normativa in materia di tutela della riservatezza dei dati personali non osta all'esercizio dei poteri di polizia giudiziaria disciplinati dal c.p.p. Spetta, tuttavia, all'Asl valutare se, nel caso di specie, l'ostensione di quanto richiesto sia impedita dal segreto professionale (richiamato nel Codice dall'art. 83), in ipotesi opponibile all'autorità giudiziaria procedente ai sensi e per gli effetti dell'art. 256 c.p.p., sull'applicazione del quale il Garante non ha competenza. Circa i requisititi delle richieste di documentazione, il Garante ha altresì precisato che, purché siano chiari la fonte ed il contenuto dei poteri esercitati, i trattamenti effettuati dalla polizia giudiziaria per attività di indagine o su delega dell'autorità giudiziaria non richiedono una compiuta informativa, comprensiva di tutti gli elementi indicati nell'art. 13 del Codice; del resto, alcune informazioni potrebbero essere non ostensibili, in considerazione di eventuali esigenze di segreto investigativo (329 c.p.p.), la cui violazione è sanzionata penalmente (art. 326 c.p.) (nota del 16 ottobre 2015).

5.1.4. La tutela della dignità della persona

Anche nel 2015 l'Autorità ha prestato particolare attenzione riguardo al trattamento dei dati personali delle donne che decidono di partorire in anonimato con specifico riferimento alla tutela della loro dignità e riservatezza (art. 30, comma 1, d.P.R. n. 396/2000). Sono pervenute, infatti, molte richieste di chiarimenti e alcune segnalazioni in merito al trattamento dei dati personali delle madri che al momento del parto si sono avvalse del diritto di non essere nominate, con particolare riferimento agli effetti della sentenza della Corte costituzionale del 18 novembre 2013, n. 278 sul quadro normativo vigente. Più precisamente, è stato segnalato che talune agenzie di servizi, presumendo l'immediata esecutività della suddetta sentenza, hanno avviato iniziative commerciali per la ricerca delle origini biologiche dei figli nati da donne che si sono avvalse del diritto di partorire in anonimato. In altri casi, sono state più genericamente rappresentate all'Autorità talune iniziative di organi giudiziari, attivati su istanza del figlio biologico, volte a contattare la madre che aveva scelto di non essere nominata nella dichiarazione di nascita.

Al riguardo, l'Autorità ha avviato alcune attività istruttorie nei confronti di strutture sanitarie e agenzie di servizi, anche mediante accertamenti ispettivi, che non hanno evidenziato specifiche criticità relativamente al trattamento dei dati personali in questione. In materia si evidenzia che il Garante ha già inviato una lettera al Presidente della Commissione giustizia della Camera dei deputati in merito alle proposte di legge in materia di anonimato materno, con particolare riferimento alle disposizioni in materia di accesso del figlio adottato non riconosciuto alla nascita, alle informazioni sulle proprie origini e sulla propria identità (segnalazione del 25 settembre 2014). In tale circostanza è stato evidenziato come la sentenza della Corte costituzionale non abbia scalfito il diritto alla riservatezza delle madri che al momento del parto si sono avvalse del diritto di non essere nominate, non avendo la pronuncia interessato il menzionato art. 30, d.P.R. n. 396/2000 ed avendo, al contrario, la Corte ribadito la necessità di proteggere in termini rigorosi il diritto all'anonimato delle donne "attraverso un procedimento, stabilito dalla legge, che assicuri la massima riservatezza" delle stesse. Solo un organico intervento del legislatore può assicurare che il diritto dei figli a conoscere le proprie origini biologiche non vada a completo detrimento della riservatezza delle donne.

Tutele alla conoscibilità dei dati sanitari

Con specifico riferimento alle segnalazioni pervenute in ordine al mancato rispetto delle misure poste a tutela della riservatezza e della dignità della persona nell'erogazione della prestazione sanitaria e nello svolgimento delle attività amministra-

tive a questa connesse, l'Ufficio ha richiamato le strutture segnalate all'adozione di soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute, prevedendo, ad esempio, apposite distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere (note 28 luglio e 1° ottobre 2015).

In altri casi, l'Ufficio è intervenuto in merito ai certificati rilasciati dagli organismi sanitari ai pazienti affinché questi ultimi possano produrli a terzi per fini amministrativi (ad es., al datore di lavoro per giustificare l'assenza dal lavoro). Tali certificati non devono contenere informazioni in grado di far risalire allo stato di salute dell'interessato: sono rali l'indicazione della struttura o del reparto presso cui ha ricevuto le cure, oppure il timbro recante la specializzazione dell'operatore sanitario che vi abbia provveduto (note 6 maggio e 4 novembre 2015).

Tutte le strutture sanitarie interessare dalle attività istruttorie dell'Ufficio hanno modificato i modelli di certificazione in uso, rendendoli rispettosi delle disposizioni sopra richiamate.

Merita particolare attenzione l'attività svolta con riferimento alla diffusione di immagini ed informazioni relative all'anamnesi e alla diagnosi dei pazienti di un pronto soccorso pubblicate da un medico ivi operante sul *social network Twitter*.

Le immagini pubblicate, sebbene lesive della dignità umana, non sono risultate riferibili a persone identificate o identificabile; i fatti sono srati denunciati alla Procura della Repubblica.

L'Autorità si è occupata della somministtazione e distribuzione dei presìdi sanitari presso le aziende sanitarie locali. Gli interventi hanno riguardato in particolare la necessità che le ditte aggiudicatarie della distribuzione dei suddetti presìdi siano designate responsabili del trattamento ed abbiano ricevuto idonee istruzioni in ordine al trattamento dei dati personali dei pazienti. Questi ultimi, inoltre, devono essere debitamente informati in merito alle caratteristiche del trattamento dei dati sanitari raccolti in occasione della valutazione e della scelta del presidio sanitario (nota 31 luglio 2015). In alcuni casi, a seguito dell'attività istruttoria, è stato aperto un procedimento sanzionatorio nei confronti della struttura sanitaria.

5.1.5. Il trattamento di dati personali concernente l'accertamento dell'infezione da HIV

Continuano a pervenire segnalazioni in merito al mancato rispetto delle misure a tutela della dignità e della riservatezza dei malati di HIV in occasione dell'erogazione di prestazioni sanitarie.

Al riguardo l'Ufficio ha ricordato che la l. 5 giugno 1990, n. 135 "Programma di interventi urgenti per la prevenzione e la lotta contro l'Aids", ha previsto specifiche disposizioni per la protezione del contagio professionale da HIV nelle strutture sanitarie ed assistenziali pubbliche e private, che sono state attuate con il d.m. 28 settembre 1990. In particolare, in considerazione dell'impossibilità "di identificare con certezza tutti i pazienti con infezione da HIV", il legislatore ha previsto alcune "precauzioni finalizzate alla protezione dal contagio [...], nei confronti della generalità delle persone assistite" (cfr. premesse del cit. d.m.). L'Ufficio ha, pertanto, richiamato il provvedimento 12 novembre 2009 (doc. web n. 1686068) in cui ha individuato specifiche garanzie per la raccolta d'informazioni sullo stato di sieropositività dei pazienti da parte degli esercenti le professioni sanitarie, che devono essere tenute in considerazione da tali soggetti nello svolgimento delle proprie attività professionali. In tale provvedimento il Garante ha vietato agli esercenti le professioni sanitarie di raccogliere l'informazione circa l'eventuale stato di sieropositività in fase di accettazione di ogni paziente che si rivolge a questi per la prima volta, indipen-

dentemente dal tipo di intervento clinico o dal piano terapeutico da eseguire, fermo restando che tale dato anamnestico può essere legittimamente raccolto, previo consenso informato dell'interessato, da parte del medico curante nell'ambito del processo di cura (nota 23 febbraio 2015).

In merito al rilascio del codice di esenzione dalla partecipazione al costo per le prestazioni di assistenza sanitaria previsto per le infezioni da HIV l'Autorità ha continuato a collaborare con il Ministero della salute e l'Istituto superiore di sanità, al fine di individuare idonee cautele volte a non far evincere in modo immediato l'esistenza di un'infezione da HIV dalla documentazione amministrativa necessaria all'erogazione della prestazione sanitaria da parte del Ssn. In tal senso, l'Autorità ha condiviso una lodevole iniziativa del Ministero della salute volta a far conoscere a tutti gli Assessorati della sanità delle regioni e province autonome l'esperienza della Regione Toscana relativa all'introduzione di procedure per il riconoscimento dell'esenzione più rispettose della disciplina in materia di protezione dei dati personali (note 5 marzo e 28 luglio 2015).

In occasione di alcune istruttorie l'Ufficio ha inoltre ricordato a diverse strutture sanitarie che la normativa in materia di prevenzione e lotta contro l'Aids non prevede l'anonimato del *test* per accertare l'infezione dell'HIV ma, impone precise cautele in relazione al trattamento del dato relativo all'avvenuto accertamento dell'infezione. La rilevazione statistica dell'infezione da HIV deve essere, infatti, effettuata con modalità tali che non consentano l'identificazione della persona e analogamente le analisi di accertamento di infezione da HIV nell'ambito di programmi epidemiologici è consentita soltanto su campioni di sangue resi anonimi (art. 5, l. n. 135/1990) (nota 6 febbraio 2015).

5.2. *I trattamenti di dati sanitari per fini amministrativi*

L'Autorità ha continuato ha fornire la propria collaborazione istituzionale nei confronti delle amministrazioni operanti nel settore sanitario con riferimento ai trattamenti di dati personali effettuati per finalità amministrative correlate alla cura anche con riferimento allo schema tipo aggiornato di regolamento per il trattamento dei dati sensibili e giudiziari che possono essere raccolti e utilizzati da regioni, province autonome, aziende sanitarie locali e altre strutture sanitarie facenti parte del Servizio sanitario regionale nell'ambito dello svolgimento delle relative funzioni istituzionali.

Una complessa attività istruttoria è stata inoltre svolta con riferimento ai trattamenti di dati personali effettuati dai centri unici di prenotazione (cup) delle aziende sanitarie.

In un caso l'Ufficio, a seguito di una segnalazione, ha riscontrato notevoli criticità in merito alla tipologia dei dati consultabili dagli operatori cup. In particolare gli operatori erano in grado di visualizzare informazioni relative alle prestazioni sanitarie già erogare e ai passati ricoveri del soggetto che stava usufruendo del servizio di prenotazione. Il sistema cup, inoltre, non forniva agli interessati una idonea informativa in merito al trattamento dei dati personali. Ulteriore criticità riscontrata riguardava la possibilità di accesso al sistema da parte di un numero elevato di soggetti non sempre deputati alla prenotazione delle prestazioni sanitarie pubbliche. A seguito del riscontro le aziende interessate hanno, tuttavia, prontamente modificato il sistema di prenotazione superando le predette criticità. Ulteriori attività istruttorie relative al trattamento dei dati personali effettuato dai cup sono attualmente in corso con particolare riferimento al coinvolgimento di società private delegate dalle strutture sanitarie all'attività di prenotazione telefonica delle prestazioni sanitarie.

L'Ufficio ha ricevuto numerose richieste di chiarimenti in merito alle modalità di consegna del promemoria della ricetta dematerializzata all'assistito con particolare riferimento alla possibilità di utilizzare modalità alternative a quella cartacea. Come è noto, la dematerializzazione della ricetta medica per le prescrizioni a carico del Ssn è stata introdotta con decreto del Mef del 2 novembre 2011. Il medico, a prescrizione avvenuta, rilascia all'assistito il promemoria della ricetta dematerializzata provvisto di numero ricetta elettronica (nre) e codice di autenticazione dell'avvenuta transazione. L'art. 1, comma 4, d.m. richiamato prevede che "il medico prescrittore rilascia all'assistito il promemoria cartaceo della ricetta elettronica secondo il modello riportato nel disciplinare tecnico Allegato 2. Su richiesta dell'assistito, tale promemoria può essere trasmesso tramite i canali alternativi di cui all'Allegato 1". Il menzionato decreto, dopo aver disciplinato le modalità dell'invio telematico dei dati della prescrizione al Sac (Sistema di accoglienza centrale), precisa che "porranno essere resi disponibili ulteriori canali per accedere ai servizi di cui al presente disciplinare erogati dal Sac, in modo particolare per la fruizione del promemoria da parte degli assistiti" (art. 3.5.1.) "attraverso il sito del Ministero dell'economia e delle finanze (www.sistemats.it)" (art. 4.1.).

Allo stato le modalità alternative alla stampa del promemoria cartaceo non sono state ancora individuate, tuttavia l'Autorità ha manifestato la propria disponibilità ad avviare un confronto con le amministrazioni istituzionali deputate ad intervenire in tale materia, al fine garantire che il trattamento dei dati personali degli assistiti avvenga nel rispetto della dignità e della riservatezza dell'interessato (note 2 ottobre 2015).

Con riferimento al trattamento dei dati personali effetruato nell'ambito dello svolgimenro delle funzioni amministrative nel settore sanitario, un importante intervento del Garante ha riguardato la trasmissione telematica delle certificazioni mediche legate alla gravidanza all'Inps. Il Garante ha infatti chiesto maggiori tutele a garanzia delle lavoratrici madri nel parere espresso su uno schema di decreto interministeriale elaborato dal Ministero del lavoro e delle politiche sociali che detta le modalità tecniche per la predisposizione e l'invio all'Inps dei certificati medici di gravidanza, interruzione della gravidanza e parto (provv. 4 giugno 2015, n. 334, doc. web n. 4130998).

Lo schema di decreto, che ha recepito molte delle indicazioni fornite dall'Ufficio nel corso di incontri avuti con le amministrazioni interessate, presenta ancora dei profili che devono essere ulteriormente perfezionati. Secondo l'Autorità lo schema deve essere integrato prevedendo che l'invio telematico dei certificati, come stabilito dalla normativa, non sia automatico, ma avvenga su richiesta della lavoratrice per consentirle di potersi avvalere dei diritti che l'ordinamento le riconosce (inrerruzione della gravidanza, non riconoscimento del figlio, parto in anonimato). Occorre, infatri, scongiurare il rischio che si instauri la prassi dell'invio automatico dei certificati senza verificare che la donna sia una lavoratrice e che voglia avvalersi dei benefici erogati dall'Inps. Nello schema inoltre, deve essere inserita una specifica disposizione che preveda l'adozione di idonee misure di sicurezza a protezione dei dari. Particolare attenzione poi, deve essere, riservata ai dati che possono essere inclusi nei certificati, evitando per esempio le diciture che possono risultare generiche o ambigue o che possono arrecare lesioni alla riservatezza delle lavoratrici.

Ulteriori modifiche richieste dal Garante riguardano il perfezionamento dello schema per evitare che il datore di lavoro venga a sapere informazioni che non deve conoscere quali l'individuazione, anche per categorie, delle strutrure sanitarie competenti all'invio dei certificati.

Procreazione medicalmente assistita

All'esito dell'esame di alcune segnalazioni, l'Ufficio è intervenuto in merito alla procreazione medicalmente assistita (di seguito pma) e, in particolare, sulle modalità di raccolta, da parte del Centro nazionale trapianti (di seguito Cnt), di dati ana-

grafici e sanitari, riferiti ai donatori di gameti destinati alla fecondazione eterologa presso le strutture sanitarie autorizzate al prelievo e al trattamento di cellule riproduttive (quali il codice fiscale, il luogo e la data di nascita, la nazionalità di origine, la cittadinanza, la provincia di residenza, lo stato civile, il titolo di studio, la condizione professionale e la posizione professionale dei donatori).

La raccolta dei dati in questione era stata disposta in attuazione della legge istitutiva del Registro nazionale dei donatori di cellule riproduttive per la fecondazione eterologa che è volto a garantire la tracciabilità del percorso delle cellule riproduttive dal donatore al nato e viceversa, nonché il conteggio dei nati generati dalle cellule riproduttive di un medesimo donatore. Queste disposizioni prevedono, inoltre, che, in attesa della piena operatività del Registro nazionale informatizzato nel quale saranno registrati tutti i soggetti ammessi alla donazione, mediante l'attribuzione di un codice identificativo ad ogni donatore – i dati riferiti ai donatori di gameti siano comunicati al Cnt "in modalità cartacea, salvaguardando comunque l'anonimato dei donatori" (art. 1, comma 298, l. 23 dicembre 2014, n. 190).

Nell'ambito di diverse interlocuzioni intercorse con il Cnt, l'Ufficio ha contribuito a individuare le misure di sicurezza necessarie e le garanzie adeguate a tutelare l'anonimato dei donatori nella fase transitoria di raccolta delle informazioni in modalità cartacea. All'esito di tale attività, il Centro ha, infatti, rivisto e modificato le procedure utilizzate per la raccolta dei dati personali dei donatori di gameti, al fine di conformarle ai principi e alle regole in materia di protezione dei dati personali.

In particolare, nella trasmissione dei dati al Cnt, sarà utilizzato dai centri di pma un codice identificativo, generato da un algoritmo di cifratura, in modo da non consentire di ricondurre i dati ricevuti alle persone cui questi si riferiscono e da permettere soltanto ai centri di identificare i donatori, qualora ne emerga la necessità per motivi di tutela della salute del donatore o dei nati. Inoltre, dalla scheda cartacea di raccolta dei dati, saranno espunte le informazioni che identificano in chiaro i donatori, mentre i dati riferiti ai donatori e ai nati, destinati a essere memorizzati nel Registro, saranno associati al predetto codice identificativo (nota 10 novembre 2015).

Registri tumori

In risposta a un quesito riguardante la liceità della trasmissione a un'Asl, che ne aveva fatto richiesta, dei dati sanitari, riferiti ad alcuni esami clinici effettuati da pazienti oncologici per l'implementazione del registro tumori aziendale, l'Ufficio ha chiarito, che qualora una struttura sanitaria intenda comunicare dati attinenti alla salute a soggetti diversi dall'interessato per finalità di carattere amministrativo, correlate ad attività di tutela della salute, tale operazione è consentita, solo se autorizzata da espressa disposizione legislativa o regolamentare che specifichi i tipi di dati che possono essere trattati e di operazioni eseguibili, nonché persegua una delle finalità di rilevante interesse pubblico individuate dalla legge (artt. 20 e 85 o 98 del Codice) (nota 23 ottobre 2015).

Pertanto, in questi casi, occorre fare riferimento alle previsioni (normative) regionali di settore eventualmente adottate, anche in attuazione del quadro di garanzie introdotto dalla normativa nazionale in materia di sistemi di sorveglianza e registri di patologia (cfr. art. 12, commi 10 ss., d.l 18 ottobre 2012, n. 179 conv., con modificazioni dalla l. 17 dicembre 2012, n. 221 e provv. 23 luglio 2015, n. 435, doc. web n. 4252386). Altrimenti la predetta verifica dovrà essere effettuata alla luce del regolamento sul trattamento dei dati sensibili e giudiziari di competenza delle aziende sanitarie, che la regione avrebbe dovuto adottare in conformità allo schema tipo su cui il Garante ha espresso il proprio parere favorevole il 26 luglio 2012 (provv. n. 220, doc. web n. 1915390, cfr. in particolare, la scheda n. 39 dell'allegato B al cit. schema tipo).

Sempre con riferimento ai registri di patologia, è proseguita l'attività di collaborazione dell'Ufficio 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 di patologia su base regionale, quali, ad esempio, quelli dei tumori (nota 8 settembre 2015).

5.2.1. L'attività consultiva sugli atti regolamentari e amministrativi del Ministero della salute

Nell'ambito dell'attività consultiva obbligatoria concernente gli atti regolamentari e amministrativi suscettibili di incidere sulla protezione dei dati personali, il Garante ha espresso, inoltre, il proprio parere su diversi decreti del Ministero della salute riguardanti temi di grande rilevanza, che coinvolgono il trattamento di dati sulla salute, raccolti in ambito sanitario in maniera sistematica e tenuti in grandi banche dati o registri a copertura nazionale o regionale, oppure idonei a rivelare lo stato di salute dei donatori di organi e di coloro che li ricevono o ancora trattati per la diagnosi precoce, in età neonatale, di malattie metaboliche ereditarie, ivi comprese quelle genetiche (cfr. par. 3.4.1).

Interconnessione dei sistemi informativi sanitari

In questo quadro, l'Autorità si è espressa su uno schema di regolamento del Ministero della salute sulle procedure per l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Ssn, anche quando gestiti da diverse amministrazioni dello Stato (provv. 19 marzo 2015, n. 162, doc. web n. 3869889).

La materia è particolarmente rilevante in quanto la prevista interconnessione comporta la raccolta centralizzata, nell'ambito del Nuovo sistema informativo sanitario (Nsis), di una notevole quantità di informazioni personali degli assistiti, particolarmente delicate, trattandosi di dati sensibili idonei specialmente a rivelare, anche nel dettaglio, lo stato di salute.

Il complesso delle informazioni, che confluiranno nel nuovo sistema centralizzato, su base individuale, ma in forma codificata, consentirà al Ministero, alle regioni e alle province autonome di valutare gli esiti delle prestazioni assistenziali, di monitorare i livelli essenziali e uniformi di assistenza e di programmare l'attività sanitaria (v. art. 15, comma 25-*bis*, d.l. 6 luglio 2012, n. 95, convertito, con modificazioni, dalla l. 7 agosto 2012, n. 135). I sistemi informativi coinvolti nelle procedure di interconnessione sono quelli del Ministero della salute previsti nell'ambito del Nsis (ad es., ticoveti, assistenza domiciliare, schede di dimissioni ospedaliere, vaccinazioni, etc.), il sistema informativo Tessera sanitaria del Ministero dell'economia e delle finanze (riguardo alle prestazioni di specialistica ambulatoriale e di assistenza farmaceutica convenzionata), nonché i sistemi informativi sanitari delle regioni e delle province autonome (limitatamente ai dati raccolti nell'ambito dei flussi del Nsis).

Per consentire l'interconnessione a livello nazionale, nell'ambito del Nsis, dei sistemi informativi sopra menzionati, lo schema di regolamento definisce le procedure per l'anonimizzazione dei dati individuali presenti nei flussi informativi del Ssn, prevedendo l'assegnazione a ciascun assistito di un codice univoco a livello nazionale, in sostituzione del codice fiscale, che non consente alcuna correlazione immediata con i dati anagrafici dell'interessato, in modo da tutelare la sua identità nel procedimento di elaborazione dei dati (art. 35, d.lgs. 23 giugno 2011, n. 118).

Lo schema di regolamento, su cui il Garante si è pronunciato con un parere favorevole condizionato, è stato elaborato dal Ministero della salute a seguito di una complessa attività, che ha coinvolto anche l'Autorità attraverso riunioni e interlocuzioni, volte a innalzare i livelli di protezione prospettati per i dati sanitari e ad indicare misure e caurele per la loro messa in sicurezza.

Le indicazioni dell'Ufficio hanno riguardato, in particolare: la definizione di procedure e modalità del trattamento in grado di assicurare adeguate garanzie a tutela della riservatezza degli assistiti, specie con riferimento al sistema informativo delle schede di dimissione ospedaliera (Sdo), per il quale sussistono particolari esigenze che richiedono un'applicazione graduale del sistema di codifica univoco previsto a livello nazionale; la precisazione dei limiti e delle modalità di accesso alle informazioni rese disponibili dal sistema Nsis, secondo un approccio selettivo e coerente con i princìpi di necessità e di indispensabilità; la razionalizzazione e l'implementazione delle misure a protezione dei dati e dei sistemi, al fine di garantire un livello di sicurezza adeguato al volume significativo e all'estrema delicatezza dei dati trattati (ad es., è stato previsto il ricorso a strumenti di autenticazione forte degli utenti per i trattamenti che prevedono l'accesso a dati sanitari riferiti a singoli individui).

Schede di dimissione ospedaliera

L'Autorità si è poi espressa su un altro schema di decreto del Ministero della salute che regola l'adeguamento della disciplina riguardante i flussi informativi dei pazienti dimessi dagli istituti di ricovero pubblici e privati (d.m. 27 ottobre 2000, n. 380) alle esigenze di monitoraggio, valutazione e pianificazione della programmazione sanitaria. Tale adeguamento trae origine anche dagli orientamenti definiti al riguardo dalla normativa dell'Unione europea che sono stati recepiti nel nostro ordinamento con il d.lgs. 4 marzo 2014, n. 38 (v. direttiva 2011/24/UE, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera e direttiva 2012/52/UE, comportante misure destinate ad agevolare il riconoscimento delle ricette mediche emesse in un altro Stato membro).

Sebbene il decreto abbia recepito talune delle osservazioni e dei rilievi formulati dall'Autorità all'esito di un tavolo tecnico con il Ministero, il Garante ha sottolineato l'esigenza di apportare al testo ulteriori perfezionamenti. Ciò, in ragione della complessità della materia e delle implicazioni riguardanti il trattamento dei dati sanitari degli assistiti e, in misura minore, di quelli giudiziari, nonché dello stretto collegamento delle previsioni del decreto con lo schema di regolamento sull'interconnessione dei sistemi informativi appena citato.

L'intervento dell'Autorità, ha consentito, tra l'altro, di estendere (a regime) al flusso informativo delle Sdo le cautele relative all'utilizzo di un codice univoco nazionale dell'assistito, previste dallo schema di regolamento sull'interconnessione dei sistemi informativi nell'ambito del Nsis, in attuazione dell'art. 35, d.lgs. n 118/2011 (la cui entrata in vigore è successiva al d.m. n. 380/2000). Tale disposizione, infatti, prevede l'anonimizzazione dei dati individuali presenti nei flussi informativi della sanità, proprio per esigenze di protezione dei dati personali, senza peraltro contemplare alcuna deroga per il flusso informativo Sdo (cfr. art. 11, comma 4, d.lgs. n. 38/2014 laddove richiama l'osservanza dell'art. 15, comma 25-*bis*, d.l. n. 95/2012).

Nel parere, inoltre, il Garante ha chiesto al Ministero di modificare le previsioni del decreto che disponevano la raccolta in chiaro nelle Sdo dei dati identificativi dei chirurghi e degli anestesisti degli interventi principali e secondari, prevedendo l'adozione di accorgimenti e misure volte sostituire il codice fiscale degli interessati con un codice univoco a livello nazionale, in analogia a quanto previsto per il trattamento del codice identificativo dei pazienti.

All'esito delle risultanze istruttorie e alla luce di una lettura del quadro normativo vigente correttamente orientata al rispetto della direttiva 95/46/CE (richiamata peraltro dalla stessa direttiva 2011/24/UE), non è emersa infatti la necessità per gli uffici del Ministero di trattare i codici fiscali dei professionisti (dai quali si possono facilmente identificare gli interessati) per monitorare e valutare gli esiti degli interventi sanitari la definizione degli *standard* di qualità, l'efficacia ed efficienza, non-

ché per monitorare il rischio clinico previsto dall'art. 11, comma 4, d.lgs. n. 38/2014 e dalla normativa europea che quest'ultima previsione intende attuare. Infine, l'Autorità ha richiamato l'attenzione del Ministero sulla necessità di limitare la raccolta dei dati contenuti nelle Sdo a quelli strettamente indispensabili, tenendo in considerazione l'esigenza che i dati oggetto di trasmissione siano conformi a quelli contenuti negli altri flussi previsti nell'ambito del Nsis, (si fa riferimento in particolare alle informazioni riferite alla data di nascita completa e al comune di nascita del paziente che non sono contemplate nei flussi informativi previsti nell'ambito del Nsis).

Per quanto riguarda invece le misure di sicurezza, in analogia a quanto previsto nello schema di regolamento sull'interconnessione dei sistemi informativi, è stato richiesto di ricorrere a strumenti di autenticazione forte per gli utenti del sistema che effettuano trattamenti particolarmente delicati, nonché di circoscrivere i casi in cui è consentito a questi ultimi di accedere ai dati sanitari riferiti a singoli pazienti dimessi dagli istituti di ricovero (provv. 26 marzo 2015, n. 178, doc. web n. 3878687).

Sistemi di sorveglianza e registri

Sempre in tema di sistemi informativi sanitari, il Garante ha reso il parere su uno schema di d.P.C.M. riguardante i sistemi di sorveglianza e i registri, ai sensi dell'art. 12, comma 11, d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla l. 17 dicembre 2012, n. 221 (provv. 23 luglio 2015, n. 435, doc. web n. 4252386).

Lo schema in questione, individua i sistemi di sorveglianza e i registri di mortalità, di tumori e di altre patologie, "di rilevanza nazionale e regionale", quelli "già disciplinati dalla normativa vigenre a livello nazionale" e quelli "di rilevanza esclusivamente regionale" precisandone le finalità, in aderenza con il dettato normativo sopra richiamato (segnatamente prevenzione, diagnosi, cura e riabilitazione, programmazione sanitaria, verifica della qualità delle cure, valutazione dell'assistenza sanitaria e ricerca scientifica in ambito medico, biomedico ed epidemiologico; cfr. art. 12, comma 10, d.l. n. 179/2012).

Sulla base del quadro notmativo vigente sopra richiamato, la definizione delle garanzie per il trattamento dei dati personali contenuti nei predetti sistemi e registri è demandata ad un regolamento da adottarsi su proposta del Presidente del Consiglio dei ministti, acquisito il parere del Garante, in conformità alle disposizioni di cui agli artt. 20, 22, e 154 del Codice (cfr. art. 13, comma 2, d.l. 21 giugno 2013, n. 69, convertito dalla l. 9 agosto 2013, n. 98 e art. 12, comma 13, d.l. n. 179/2012). Poiché non è risultato che tale atto sia stato adottato, l'Autorità ha innanzitutto richiamato l'attenzione sulla necessità che il predetto regolamento venga predisposto quanto prima al fine di rendere leciti e rispettosi di adeguate cautele i trattamenti di dati sensibili effettuati in tale ambito.

In ragione della particolare delicatezza della materia (art. 94 del Codice) al fine di registrare e caratterizzare tutti i casi di rischio per la salute di una particolare malattia o di una condizione di salure rilevante in una popolazione definita, il Garante ha condizionato il proprio parere favorevole al recepimento di una serie di indicazioni volte a rendere conforme il testo del regolamento alla disciplina in materia di protezione dei dati personali.

Tali osservazioni hanno riguardato, in parricolare, la verifica dell'idoneità dei presupposti legittimanti l'utilizzo a fini di cura dei dati contenuti nei sistemi di sorveglianza e nei registti, al fine di scongiurate trattamenti illeciti di dati e un utilizzo improprio degli archivi in questione (quasi fossero fascicoli sanitari elettronici accessibili, però, in assenza delle specifiche cautele previste per questi ultimi; cfr. art. 12, commi 1-7, d. l. n. 179/2012). Al riguardo, va tenuto in considerazione, infatti, che il trattamento di dati sulla salute per le predette finalità può essere legittimamente effettuato soltanto da organismi sanitari e da esercenti la professione sanitaria, nel

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 perlopiù 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).

Qualità e sicurezza del sangue e degli emocomponenti

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 (provv. 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 Pallidium).

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

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 diretriva 2012/25/UE sullo scambio tra Stati membri di tali organi (provv. 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 renga anche in considerazione l'esigenza di garantire la qualità, la disponibilità e la non disconoscibilità degli stessi dati.

Lo schema di decrero 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.

Screening neonatale

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 (provv. 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 particolate 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 i 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.

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 rrasferiti (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 possibilirà 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 dari, 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).

Biobanche a fini di ricerca

Nel corso dell'anno è stato affrontato il rema 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-

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. 6.1*a*) 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. *l*) 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'ordimento 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 srara 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-

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

Servizi personalizzati di prevenzione medico-genetica *online*

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 finalirà 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 giustificherebbero l'accoglimento della richiesta (note 6 maggio e 3 luglio 2015).

Osservatorio regionale antiviolenza

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-

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).

Piano d'azione straordinario contro la violenza di genere

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).

Trasferimento all'estero di dati di farmacovigilanza

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 (provv. 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*

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

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 (Anncsu) (provv. 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'Anncsu 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 trattamenti 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'Anncsu – 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 successi 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.

Programma statistico nazionale (Psn)

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).

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, sni qnali 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'Antorità 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 rilevanri 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 nnivoci 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'inrera 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 consentira 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), inseriro 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 Anncsu.

Il Garante he 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, e 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 ptedisposti 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 rivelate 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 quesrionario.

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*

Videosorveglianza nelle carceri

Nel 2015 sono giunte diverse segnalazioni relative all'istallazione 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. 165/2011) "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-

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 conttollo 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).

Sperimentazione di microcamere

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).

Videoriprese per servizi giornalistici

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

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 (riporrato 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).

Dati giudiziari nel verbale di revisione delle dichiarazioni doganali

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).

Dati sensibili delle detenute di una casa circondariale

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 morre 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.

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 considetare con riferimento all'arr. 11 del Codice (provv. 1° ottobre 2015, n. 507, doc. web n. 4429647).

Comunicazioni delle assenze per malattia in una casa circondariale

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 dipendenre, di non ptendere servizio "per malore" 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

casi, (quando segue la precisazione che l'assenza è per malattia), dati di natura sensibile. Infatti, secondo il costante orientamento del Garante (di recente provv. 10 ottobre 2013, n. 442, doc. web n. 2753605, nonché, negli stessi termini v. provv. 14 giugno 2007, n. 23, doc. web n. 1417809, recante Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, punto 6.3, e Corte di Cassazione 8 agosto 2013, n. 18980) costituisce dato sensibile quello relativo all'assenza dal lavoro di un dipendente per malattia, in quanto tale informazione, pur non facendo riferimento a specifiche patologie, è comunque suscettibile di rivelare lo stato di salute dell'interessato. Pertanto, il Garante ha valutato che l'attribuzione al personale di portineria del trattamento dei dati personali – sensibili e non – degli agenti di polizia penitenziaria in assenza di nomina ad incaricato del trattamento e di definizione dell'ambito di trattamento consentito, configura la violazione dell'art. 30 del Codice (provv. 7 maggio 2015, n. 269, doc. web n. 4167648).

8.3. *Il controllo sul sistema di informazione Schengen*

Il Ministero dell'interno-Dipartimento della pubblica sicurezza, anche per il 2015, ha rappresentato l'opportunità di differire l'adempimento delle misure non ancora attuate, tra quelle prescritte dal Garante per rafforzare la sicurezza nel trattamento dei dati effettuati per l'attuazione della Convenzione di Schengen, in ragione sia delle innovazioni tecnologiche 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. Nel corso dell'anno il Ministero ha peraltro fornito ulteriori elementi, che sono allo stato al vaglio dell'Autorità, circa l'idoneità delle misure poste in essere a soddisfare le prescrizioni impartite.

Su altro profilo, com'è noto il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nel SIS II, in virtù dei quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale dell'archivio Schengen, ossia al Dipartimento della pubblica sicurezza (cd. accesso diretto).

Il numero ed il contenuto delle richieste degli interessati che ancora pervengono direttamente al Garante hanno pertanto, anche quest'anno, subito un lieve calo rispetto all'anno precedente.

Sono invece in lieve aumento le richieste di accesso prevenute al Garante da autorità nazionali di controllo di altri Stati, interpellare dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane. Le informazioni sono state comunicare, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni di cui all'art. 62, decisione 2007/533/GAI del Consiglio e all'art. 46 del regolamento (CE) n. 1987/2006 del Parlamento Europeo e del Consiglio (cfr. par. 22.4).

9 L'attività giornalistica

L'Autorità è intervenuta su questioni attinenti al bilanciamento fra la libertà di informazione e il diritto alla protezione dei dati personali non solo in occasione del consueto esame di segnalazioni, reclami e ricorsi ma anche mediante la predisposizione di un *report* "La televisione del dolore" presenrato dalla professoressa Licia Califano a Pavia il 24 marzo 2015.

Tale documento ha costituito un'importante occasione di riflessione sul tema e ha, in particolare, evidenziato il divario tra la normativa e il modo di fare informazione da parte di alcuni *media*, talora finalizzato alla "ricerca del sensazionalismo e di un'emotività collettiva usa e getta", attraverso l'uso di immagini e l'indugio su dettagli lesivi della dignità e della sfera privata delle persone (Consiglio nazionale dell'Ordine dei giornalisti – Osservatorio di Pavia *Media Research* – doc. web n. 3845045).

9.1. *Le persone decedute*

I minori

Non è mancata, anche nel periodo di riferimento, la necessità di richiamare gli organi di informazione al rispetto delle particolari garanzie previste per i minori.

In particolare è stata esaminata una segnalazione relativa alle puntate di un programma televisivo dedicate alle indagini concernenti il ritrovamento del cadavere di una donna lungo le rive di un canale e dell'asserita assenza di accorgimenti atti a garantire la vittima ed i suoi congiunti, in particolare i figli minori. Di questi ultimi, infatti, sono state fornite informazioni dettagliate riguardanti la loro vita privata indugiando in particolare sulle diverse ipotesi riguardanti il destino dei minori in caso di un possibile accertamento della colpevolezza del padre. L'Autorità, pur rilevando l'interesse pubblico della vicenda, ha rinvenuto nel trattamento in questione una violazione del limite dell'essenzialità dell'informazione (art. 137, comma 3, del Codice) e delle specifiche garanzie a tutela della dignità e della personalità dei minori previste dal codice di deontologia (art. 7), dalla Carta di Treviso e dalla Convenzione sui diritti del fanciullo (art. 16); conseguentemente ha chiesto all'editore, titolare del trattamenro, di impegnarsi autonomamente a non diffondere ulteriormente i dati personali relativi ai cirari minori, nonché di rimuovere quelli reperibili sulle edizioni *online* (nota 10 luglio 2015).

Gli esiti scolastici

L'Autorità ha poi ricordato che il principio di essenzialità dell'informazione non viene meno per la sola circostanza che i dati da diffondere sono soggetti a un regime di pubblicità, come accade per quelli relativi agli esiti scolastici. Tale assunto è stato richiamato in relazione all'avvenuta diffusione – anche *online* – di una riproduzione del quadro dei voti della classe di cui faceva parte un giovane, deceduto durante una gita scolastica. L'articolo consentiva di individuare i nomi e i cognomi dei compagni di classe del deceduto, associati ai voti ricevuti ivi compresi quelli relativi alla condotta. L'Autorità ha ritenuto che tali informazioni, per la loro natura e per i soggetti a cui si riferivano, nulla aggiungevano al quadro informativo sulle possibili

cause del decesso del giovane e ne ha chiesto pertanto la rimozione (nota 25 giugno 2015).

9.2. *La cronaca giudiziaria*

Vittime di reato

L'Autorità è intervenuta d'urgenza in relazione ad un articolo che, nel dare notizia del rinvio a giudizio dei presunti autori di una violenza sessuale ai danni di una donna, ha diffuso il nome e cognome di quest'ultima unitamente ad altri dati (età, nazionalità, professione del padre), nonché la descrizione particolareggiata delle violenze subire. Nel richiamare i divieti di legge operanti al riguardo (art. 734 c.p.), i limiti previsti dal Codice (art.137, comma 3) e dal codice di deontologia (artt. 6, 8 e 12) a tutela della riservatezza e della dignità della persona e i diversi provvedimenti già adottati in materia (cfr. da ultimo provv. 8 aprile 2009, doc. web n. 1610028) ha disposto il divieto di ogni ulteriore diffusione, anche *online* delle generalità della vittima della violenza descritta, nonché il divieto di diffusione di dati comunque idonei ad identificarla (provv. 18 giugno 2015, n. 358, doc. web n. 4172412).

Immagini del cadavere

Il Garante si è occupato della diffusione delle foto del cadavere di un giovane giornalista ucciso brutalmente dalla camorra nel 1985, pubblicate su un siro internet e su un libro. In particolare, il segnalanre lamentava una violazione della Carta dei doveri del giornalista, dove si dispone che questi "non deve pubblicare immagini o fotografie particolarmente raccapriccianti di soggetti coinvolti in fatti di cronaca, o comunque lesive della dignità della persona, né deve soffermarsi sui dettagli di violenza o di brutalità, a meno che non prevalgano preminenti motivi di interesse sociale" e dell'art. 15 della l. 8 febbraio 1948, n. 47 (Disposizioni sulla stampa). Il Garante ha tuttavia osservato che la pubblicazione di queste foto era giustificata dalla rilevanza sociale rivestita dalle stesse, trattandosi di un fatto di particolare gravità che ha avuto a suo tempo una vasta eco e che ancora oggi, a distanza di trenta anni dall'accadimento del fatto, viene spesso ricordato (provv. 8 ottobre 2015 n. 520, doc. web n. 4363110).

9.3. *I personaggi pubblici*

Dati relativi alla sfera sessuale

Il Garante, pur avendo riaffermato il principio in base al quale la diffusione di informazioni riguardanti personaggi pubblici o che esercitano pubbliche funzioni, pur se relative alla sfera privata, può risultare giustificata in ragione della "qualificazione del protagonista" (art. 6, comma 1, del codice deontologico), ovvero del rilievo che le informazioni medesime possono avere sul ruolo o sulla vita pubblica del soggetto cui si riferiscono (art. 6, comma 2), ha ritenuto illecita la diffusione delle descrizioni particolareggiate delle condotte sessuali di una personaggio politico riportate negli scritti confluiti negli atti giudiziari e diffusi negli articoli di stampa cartacea e *online*. Ha infatti applicato l'art. 11 del codice di deontologia, il quale stabilisce che "il giornalista si astiene dalla descrizione di abitudini sessuali riferite ad una determinata persona identificata o identificabile" e che "la pubblicazione è ammessa nell'ambito del perseguimento dell'essenzialità dell'informazione e nel rispetto della dignità della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica" (provv. 8 luglio 2015, n. 407, non pubblicato ai sensi dell'art. 24 del reg. Garante 1° agosto 2013).

Uso di artifici nelle interviste

Il Garante si è pronunciato nuovamente sulla prassi, adottata in un noto programma radiofonico, di raccogliere telefonicamente dichiarazioni di persone con l'artificio della simulazione di altra identità e successivamente di diffonderle radiofo-

nicamente, sul web o in altro modo. L'Autorità si era già pronunciata in merito con il provvedimento dell'11 settembre 2014, n. 400 (doc. web n. 3405138), ravvisando in tale fattispecie un trattamento illecito di dati personali. Il provvedimento, impugnato, è stato confermato dal Tribunale di Milano (sent. 4 giugno 2015, n. 6968). Ciononostante la prassi descritta è proseguita, sicché l'Autorità, anche alla luce di una nuova segnalazione pervenuta al riguardo, ha ritenuto necessario avviare una nuova istruttoria. Questa si è conclusa con un provvedimento di prescrizione al titolare del trattamento di astenersi dall'acquisizione di dati personali con le modalità descritte, poiché tale condotta costituisce una violazione dei principi di trasparenza e correttezza del trattamento di cui all'art. 11 del Codice e 2 del codice di deontologia.

L'Autorità ha precisato che la prassi descritta configura un vero e proprio "artificio" – non conforme alla menzionata disciplina – consistente non solo nel celare l'identità di giornalista (o soggetto ad esso equiparato ai sensi dell'art. 136 del Codice), bensì anche nell'utilizzare l'identità e la voce di un'altra specifica persona, amica dell'"intervistato" o comunque da questi conosciuta, inducendo così quest'ultimo, fraudolentemente, a manifestare considerazioni del tutto private, confidenziali (talvolta anche dati sensibili) e destinate unicamente, nell'effettivo intento dell'"intervistato", al soggetto del quale il giornalista-imitatore si è artificiosamente assunto l'identità. Ciò, nell'ambito di una conversazione telefonica rispetto alla quale l'interlocutore "intervistato" ha una legittima aspettativa di riservatezza (art. 15 Cost.) (provv. 2 dicembre 2015, n. 631, doc. web n. 4634594).

9.4. *Gli archivi storici e le informazioni* online

In conformità alla sentenza della CGUE del 13 maggio 2014 nel caso Google Spain (cfr. Relazione 2014, p. 87) il Garante è intervenuto a seguito delle segnalazioni e reclami presentate da cittadini avverso il mancato accoglimento da parte di Google delle richieste di deindicizzare pagine presenti sul web riportanti dati personali ritenuti non più di interesse pubblico. Il Garante ha seguito al riguardo i criteri adottati nelle Linee guida del Gruppo Art. 29 (parere WP 26 novembre 2014, n. 225, doc. web n. 3876849).

Tra i casi di accoglimento, si segnala quello relativo ad un articolo rinvenibile tra l'elenco dei risultati generato da Google a seguito della ricerca effettuata a partire dal nome e cognome dell'interessato riguardante i dissidi intercorsi tra il segnalante e l'autore di un *blog* in costanza di un rapporto professionale da tempo interrotto. Il Garante ha ritenuto i fatti rinvenibili nella url privi di inreresse pubblico e ne ha prescritto a Google la rimozione a partire dal nome e dal cognome del segnalante (provv. 16 aprile 2015, n. 222, doc. web n. 4006340).

Ha inoltre ritenuto di prescrivere a Google la rimozione di un articolo del 1999 che dava conto della visita effettuata dal segnalante, all'epoca deputato, a un detenuto presso un carcere nel reparto speciale riservato ai mafiosi. A seguito di tale incontro, la Procura antimafia avrebbe aperto un'indagine per verificare se la visita fosse stata effettivamente solo mirata a controllare le "condizioni generali della detenzione" come prescritto dalla legge per i parlamentari.

Il Garante ha ritenuto la lesione provocata dall'indicizzazione dell'articolo in questione sproporzionata in ragione del rilevante lasso di tempo trascorso dalla vicenda e delle dichiarazioni del segnalante secondo le quali non è stato avviato alcun procedimento penale nei suoi confronti (provv. 5 febbraio 2015, n. 64, doc. web n. 3793836).

Il Garante, invece, non ha accolto le richieste relative a controversie giudiziarie ancora in corso, di rilevanza nazionale (provv.ti 8 gennaio 2015, n. 1, doc. web n. 3730791, 16 aprile 2015, n. 224, doc. web n. 4006473 e 4 giugno 2015, n. 335 doc. web n. 4172122), strettamente connesse all'attività professionale dei reclamanti (provv. 16 aprile 2015, n. 223, doc. web n. 4006413), particolarmente efferate (provv. 16 aprile 2015, n. 225, doc. web n. 4006601) e quindi caratterizzate da un persistente interesse pubblico alla loro rinvenibilità sul motore di ricerca.

Deindicizzazione dei nominativi su atti ministeriali pubblicati su GU *online*

Il Ministero della giustizia ha riferito di avere ricevuto numerose richieste di oscuramento dei nomi di persone riportati su atti ministeriali – segnatamente decreti per riconoscimento dei titoli professionali conseguiti all'estero pubblicati nella GU *online*. In particolare gli interessati si lamentavano della circostanza che le ricerche condotte sul web mediante i comuni motori di ricerca consentivano di risalire ad atti pubblicati nella GU anche a notevole distanza di tempo. Il Garante, richiamando le Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, adottate dal Garante con provv. 15 maggio 2014, n. 243 (doc. web n. 3134436), la menzionata sentenza della CGUE e le cit. Linee guida adottare dal Gruppo Art. 29 (doc. web n. 3134436), ha rappresentato l'opportunità che l'Amministrazione, alla luce dei criteri della notorietà pubblica dell'interessato e della risalenza nel tempo dell'informazione, valuti la sussistenza di motivi che giustifichino l'indicizzazione, da parte dei motori di ricerca, dei dati personali citati nei provvedimenti pubblicati nella GU *online*, adottando, se del caso, gli accorgimenti tecnici opportuni per impedire l'indicizzazione stessa (nota 14 dicembre 2015).

10 Il trattamento di dati personali attraverso internet

10.1. *L'informativa e consenso per il trattamento dei dati personali mediante i siti web*

Come già segnalato l'anno scorso (cfr. Relazione 2014, p. 89), l'Ufficio ha ravvisato per alcuni siti web profili di parziale inidoneità in ordine ad alcune informative rilasciare ai sensi dell'art. 13 del Codice nonché con riguardo a *form* di registrazione a servizi vari per consensi non adeguatamente differenziati a seconda dei diversi trattamenti di dati indicati o, in alcuni casi, impostati in maniera da essere obbligatoriamenre resi per finalità ulteriori a quelle di servizio, ai sensi degli artt. 23 e 130 del Codice.

In materia, si segnala l'adozione del provvedimento 1° ottobre 2015, n. 508 (doc. web n. 4452896) a contenuto inibitorio e prescrittivo, adottato in relazione all'invio di messaggi promozionali indesiderati via sms ad utenti che avevano prestato il proprio consenso al solo scopo di ottenere l'iscrizione ad un servizio di candidatura *online* per la ricerca di lavoro.

Inoltre, può farsi riferimento anche al provvedimento 18 novembre 2015, n. 605 (doc. web n. 4487559) adottato nei confronti di una nota società di *e-commerce,* la quale rilasciava un'informativa priva del riferimento ad alcune operazioni di trattamento (come la profilazione e la comunicazione a terzi per finalità promozionali) che, secondo quanto accertato, effettuava e raccoglieva un consenso preselezionato e unico al trattamento dei dati (v. *amplius* par. 11.3).

10.2. *Le Linee guida in materia di trattamento di dati personali per profilazione* online

Nel mese di marzo, in coerenza con le regole emanate nei confronti di Google Inc., di cui al provvedimento 10 luglio 2014, n. 353 (doc. web n. 3283078), il Garante ha adottato un provvedimento a carattere generale volto a disciplinare l'attività dei soggetti che, offrendo servizi *online* accessibili al pubblico attraverso reti di comunicazione elettronica (i cd. servizi della società dell'informazione), effettuano anche attività di profilazione ovvero di analisi ed elaborazione di informazioni relative a utenti o clienti, al fine di suddividere gli interessati in "profili", cioè in gruppi omogenei per comportamenti o caratteristiche sempre più specifici.

L'Autorità, con l'intento di armonizzare e semplificare le regole applicabili in materia di protezione dei dati personali nell'espletamento di questa attività, generalmente strumentale sia alla messa a disposizione di servizi sempre più mirati e conformati sulle specifiche esigenze dell'utente, sia alla fornitura di pubblicità personalizzata, ha richiamato i titolari all'adempimento di specifici obblighi, ed innanzitutto quello di fornire agli utenti un'informativa chiara e completa, facilmente accessibile, preferibilmente strutturata su più livelli.

In secondo luogo, ha ricordato la necessità di richiedere ed ottenere il consenso degli interessati, revocabile in ogni momento, per la profilazione per finalità promozionali comunque effettuata: sia se relativa al trattamento, in modalità automatizzata, dei dati personali che derivano dall'utilizzo di servizi di posta elettronica; sia se fondata sull'incrocio dei dati raccolti in telazione alla fornitura ed al relativo utilizzo

di più servizi diversi tra quelli messi a disposizione dell'utente (ad es., posta elettronica e navigazione sul web, partecipazione a *social network* e utilizzo di mappe o visualizzazione di contenuti audiovisivi etc.); sia, infine, se basata sul ricorso ad altre tecniche di identificazione (credenziali di autenticazione, *fingerprinting*, etc.).

L'Autorità ha inoltre imposto modalità di trattamento idonee ad offrire concrete tutele tanto agli utenti, cd. autenticati, che accedono ai servizi tramite un *account* (ad es., per l'utilizzo della posta elettronica), quanto a quelli che ne fanno uso in assenza di preventiva autenticazione, come in caso di semplice navigazione *online*.

Pur ribadendo la libertà di scelta che compete ai titolari, le Linee guida varate dal Garante hanno fornito anche alcune indicazioni pratiche circa le misure da adottare per assicurare la conformità alla normativa dei trattamenti di dati in questione.

A tale scopo è stata, tra l'altro, identificata una possibile modalità per l'acquisizione del consenso *online* che prevede la presentazione di un *banner* all'utente attraverso il quale questi possa attivamente effettuare scelte consapevoli sul trattamento delle informazioni che lo riguardano. Si tratta di un meccanismo che, a tecnologia vigente e in una prospettiva di semplificazione, presenta vantaggi sia in termini di tutela della persona sia di salvaguardia della sua esperienza di navigazione o di accesso ad altri servizi in rete.

Da ultimo, è stato ribadito l'obbligo, che grava sui titolari, del rispetto del diritto di opposizione previsto dal Codice, nonché quello dell'adozione di una *policy* per la definizione di tempi di conservazione dei dati che risultino proporzionati alle specifiche finalità perseguite (provv. 19 marzo 2015, n. 161, doc. web n. 3881513).

10.3. *La consultazione pubblica su* Internet of Things

Con provvedimento 26 marzo 2015, n. 179 (doc. web n. 3898704), l'Autorità ha avviato una consultazione pubblica sul cd. *Internet of Things* (IoT), segnatamente sui rischi per la protezione dei dati che derivano dall'impiego sempre più generalizzato di tecniche che consentono l'interazione e l'interconnessione di oggetti e sistemi diversi (*smartphone*, *tablet* e pc, ma anche oggetti di uso quotidiano come, tra gli altri, dispositivi indossabili, di automazione domestica e di geolocalizzazione e navigazione assistita).

Gli accorgimenti tecnici utilizzati consentono infatti, per il tramite di sensori integrati negli oggetti, di registrare, processare, immagazzinare dati localmente o tramite l'interoperabilità dei dispositivi tra loro sia nel medio raggio, mediante l'utilizzo di tecnologie a radio frequenza (ad es., Rfid e *bluetooth*), sia tramite una rete di comunicazione elettronica. Ne risultano spesso vantaggi e semplificazioni d'uso per l'utente (impianti di riscaldamento che si accendono da remoto con lo *smartphone*, frigoriferi che segnalano la scadenza dei cibi, sistemi di trasporto in grado di aumentare automaticamente il numero delle corse sulla base degli accessi registrati ai tornelli, orologi intelligenti che segnalano al medico curante eventuali anomalie corporee, sistemi di allarme che si azionano in modo autonomo, luci per uso pubblico o privato che si azionano rispettando parametri di funzionalità e risparmio energetico), che tuttavia comportano la raccolta, la registrazione e l'elaborazione di una grande quantità di informazioni relative a utenti spesso inconsapevoli.

Questi dati consentono non solo di costruire profili dettagliati delle persone, basati sui loro comportamenti, abitudini, gusti e perfino sullo stato di salute, ma di effettuare anche un monitoraggio particolarmente invasivo sulla loro vita privata e di mettere in atto potenziali condizionamenti della loro libertà, peraltro basandosi

10

su informazioni delle quali non è neppure possibile garantire l'affidabilità o il trattamento nel rispetto di rigorose misure di sicurezza.

L'avvio della consultazione pubblica ha avuto l'obiettivo di effettuare una valutazione complessiva anche allo scopo di definire misure per assicurare agli utenti la massima trasparenza nell'uso dei loro dati personali e per tutelarli contro possibili abusi. In particolare, con lo strumento della consultazione pubblica, l'Autorità ha inteso acquisire elementi e proposte sulle modalità di informazione degli utenti, anche in vista di un eventuale consenso; sulla possibilità che fin dalla fase di progettazione dei servizi e dei prodotti gli operatori coinvolti adottino soluzioni tecnologiche a garanzia della *privacy* degli utenti (in un'ottica di cd. *privacy by design*); sul ricorso a tecniche di cifratura e anonimizzazione delle informazioni; sulla interoperabilità dei servizi e sugli aspetti di standardizzazione necessari per garantirla; sull'adozione di strumenti di certificazione.

Conclusa, nel novembre 2015, la fase di acquisizione dei contributi, è attualmente in corso la loro valutazione da parte dell'Autorità.

11 Il trattamento di dati personali nel settore delle comunicazioni elettroniche

11.1. *Le telefonate promozionali indesiderate*

Anche nell'anno di riferimento l'Autorità ha dovuto svolgere complesse attività istruttorie per contrastare il fenomeno delle chiamate indesiderate. Ciò, in quanto il flusso delle segnalazioni pervenute è, rispetto agli anni precedenti, ulteriormente cresciuto. Innanzitutto, per determinate la riconducibilità delle chiamate agli effettivi autori delle telefonate in questione, si è dovuto procedere a degli specifici accertamenti. Tale indagine è stata assai più complessa nei numerosissimi casi in cui le chiamate sono state fatte mediante l'oscuramento delle numerazioni chiamanti. Inoltre, dalle suddette verifiche si è constatato che le aziende pubblicizzanti i prodotti si sono avvalse, oltre che del proprio personale, anche di agenzie esterne le quali a loro volta hanno demandato l'operato a terzi soggetti a volte anche stabiliti all'estero. Al riguardo, nel corso di alcuni accertamenti ispettivi presso le aziende committenti, nonché in occasione di riunioni in sede con alcuni gestori telefonici, è stato riscontrato che le filiere di soggetti cui vengono demandate le attività di *telemarketing* sono talmente diramate per l'uso ripetuto di agenzie e *sub* agenzie da non consentire sempre agli stessi soggetti mandanti il controllo della struttura e diventando quindi difficile risalire a coloro che materialmente hanno effettuato i contatti telefonici lamentati, nonché alle numerazioni chiamanti.

Come sopra evidenziato, il fenomeno del cd. oscuramento ha assunto, nel tempo, dimensioni sempre più considerevoli in materia di *telemarketing* "selvaggio". L'impossibilità, per l'utente, di indicare la numerazione chiamante nelle segnalazioni ha reso difficile, in tali casi, l'individuazione del titolare e quindi l'accertamento della sussistenza della violazione della disciplina relativa alla protezione dei dati personali.

L'Autorità ha dunque deciso di affrontare tale fenomeno adottando misure più rigorose nell'ambito dei poteri che le sono attribuiti dal Codice riuscendo a risalire ai numeri chiamanti nonostante l'oscuramento.

Si segnala in particolare l'adozione di un provvedimento di divieto e prescrittivo nei confronti di una società di *telemarketing* (provv. 1° ottobre 2015, n. 503, doc. web n. 4449190). Si tratta del caso di un utente che lamentava di essere stato disturbato con offerte promozionali nonostante il proprio numero non fosse presente, come da sua richiesta, in alcun elenco telefonico (cd. utenza riservata). Il segnalante non possedeva un dispositivo che consentisse la visualizzazione del numero da cui lo contattavano i promotori commerciali e aveva potuto fornire all'Autorità solo generiche indicazioni sulle chiamate ricevute. Per poter accertare i fatti segnalati, il Garante ha dovuto quindi avviare diverse verifiche con più operatori telefonici che hanno permesso di risalire alla numerazione chiamante, riconducibile a una società di *telemarketing* nei confronti della quale è poi stato adottato il suddetto provvedimento unitamente alla società committente.

Si rappresenta, infine, che numerose istruttorie avviate sono state definite con la contestazione di sanzioni nei confronti sia delle società committenti, sia di quelle delegate direttamente o indirettamente all'effettuazione di attività di *telemarketing*.

11.2. *I trattamenti di dati personali effettuati mediante* call center *ubicati al di fuori dell'Unione europea*

A seguito delle prescrizioni impartite con il provvedimento 10 ottobre 2013, n. 444 (doc. web n. 2724806), sono pervenute al Garante nel 2015 diverse notificazioni di trasferimento o affidamento all'estero del trattamento di dati personali per servizi di *call center*.

Inoltre è proseguita l'attività ispettiva già avviata negli anni scorsi, in collaborazione con il Nucleo speciale *privacy* della Guardia di finanza, per verificare la liceità dei trattamenti posti in essere dai titolari che si avvalgono di *call center* esteri. Sono state sottoposte ad accertamento ispettivo 29 società, tra titolari del trattamento e *call center* che operano in qualità di responsabili. Ne è emerso un quadro di sostanziale conformità alla disciplina.

Inoltre, il Garante e la competente Istituzione albanese hanno siglato il 10 febbraio 2015 un Accordo di cooperazione allo scopo di assicurare la tutela dei dati personali dei cittadini italiani e albanesi raccolti e utilizzati da soggetti pubblici e privati che operano in Albania, dove negli ultimi anni molte aziende italiane hanno fatto richiesta di servizi di *call center*.

La cooperazione prevede un'attività ispettiva congiunta presso pp.aa. e aziende private, inclusi i *call center* che operano in Albania (doc. web n. 3733348).

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

In materia di *marketing* e profilazione, con specifico riferimento ai trattamenti di dati effettuati da una società fornitrice del servizio di posta elettronica certificata, l'Autorità ha vietato il trattamento dei dati personali raccolti al momento della sottoscrizione del contratto relativo alla richiesta di attivazione del servizio di posta elettronica certificata, per ulteriori finalità (quali quelle promozionali, di profilazione e comunicazione a soggetti terzi autonomi titolari del trattamento), poiché non conforme a quanto previsto dagli artt. 23 e 130 del Codice. Inoltre, ha prescritto di adottare, qualora intenda raccogliere dati personali degli interessati ed utilizzarli per finalità di definizione del profilo dell'utente e/o di promozione commerciale, le misure necessarie ed opportune al fine di rendere i trattamenti dei dati personali conformi alla normativa in materia e, in particolare, l'acquisizione di specifici consensi al trattamento dei dati personali per ciascuna distinta finalità eterogenea. Si evidenzia altresì che l'Autorità ha prescritto, per quanto riguarda il *form* di contatto per la richiesta d'assistenza, l'eliminazione di qualsivoglia meccanismo di subordinazione dell'esito della procedura alla prestazione di un consenso per il trattamento di dati personali a fini promozionali o di definizione del profilo dell'utente e, qualora intenda utilizzare i dati otrenuti per le comunicazioni di cui all'art. 130, comma 4, del Codice, l'adeguamento alle previsioni di quest'ultimo (ossia il cd. "*soft spam*"). È stato chiesto infine di inserire nell'informativa relativa al *form* un chiaro ed espresso riferimento all'art. 130, comma 4, del Codice ove intenda trattare i dati ottenuti in conformità a tale disposizione, specificando, altresì, le diverse finalità perseguite e chiarendo il tipo di modalità di comunicazione promozionale utilizzata (automatizzata e non automatizzata) (provv. 13 maggio 2015, n. 291, doc. web n. 4337465).

L'Autorità inoltre è intervenuta nei confronti di una delle più importanti società di fornitura *online* di biglietti per spettacoli teatrali, manifestazioni sportive, concerti, nonché di *e-commerce* di prodotti anche di marchi celebri. Dagli accertamenti

ispettivi svolti è emerso che la società raccoglieva dati personali attraverso tre siti web, di cui uno operativo in più lingue straniere destinato ad utenti di Paesi UE ed *extra*-UE, talora richiedendo un consenso preselezionato e unico per varie finalità, fra cui quelle di *marketing*, profilazione, nonché comunicazione dei dati ad altre società, per le loro autonome finalità commerciali. In particolare, la società svolgeva un'attività di profilazione utilizzando un *software* per l'invio di *newsletter* personalizzate, "create" elaborando i dati relativi agli ordini dei clienti o anche a prodotti inseriti nel carrello il cui ordine non era stato comunque finalizzato, senza aver provveduto a notificare all'Autorità siffatto invasivo trattamento.

Il Garante, pertanto, ha vietato alla stessa, ai sensi dell'art. 23 del Codice, l'illecito trattamento dei dati personali di oltre trecentomila clienti, altresì prescrivendole di integrare l'informativa, resa *online*, indicando le aziende o le categorie economiche o merceologiche, alle quali intende comunicare i dati per finalità promozionali. Ha inoltre prescritto alla medesima società di avvisare le aziende, alle quali i dati erano stati comunicati o ceduti, di non utilizzarli senza il consenso degli interessati, nonché di prevedere tempi di conservazione dei dati e di provvedere all'immediata cancellazione o alla anonimizzazione permanente degli stessi alla scadenza del termine di conservazione (provv. 18 novembre 2015, n. 605, doc. web n. 4487559).

11.4. *Le verifiche preliminari* ex *art. 17 del Codice*

Il Garante nel corso dell'anno ha analizzato e dato riscontro a più verifiche preliminari presentate da titolari del trattamento afferenti a diversi settori produttivi, ossia a specifiche istanze volte a individuare misure ed accorgimenti idonei ad assicurare la correttezza e la liceità dei trattamenti prima della loro effettuazione, in considerazione dei rischi specifici per il diritto alla protezione dei dati personali degli interessati.

I mutamenti registrati nel mercato della telefonia ed in particolare la crescente richiesta di servizi personalizzati, sotto il profilo dei contenuti e del piano tariffario, hanno indotto alcuni fornitori di servizi di comunicazione elettronica accessibili al pubblico a richiedere all'Autorità, attraverso istanze di verifica preliminare (*ex* art. 17 del Codice), l'autorizzazione allo svolgimento di ulteriori trattamenti di dati personali aggregati della propria clientela per finalità di profilazione, previo esonero dall'acquisizione del consenso specifico degli interessati (*ex* art. 24, comma 1, lett. *g*) del Codice), ferma restando la necessaria acquisizione del consenso preventivo degli stessi per la successiva attività di *marketing* diretto (art. 23 del Codice).

Settore telefonico

Tenuto conto dei provvedimenti generali 25 giugno 2009 (doc. web n. 1629107) e 6 febbraio 2014 (doc. web n. 2951718), nonché degli specifici provvedimenti emanati in tale ambito a seguito di precedenti istanze di *prior checking*, il Garante ha adottato due provvedimenti prescrittivi nei confronti di due operatori telefonici coinvolti, stabilendo una serie di misure giuridiche e di accorgimenti tecnici volti a garantire il corretto trattamento dei dati personali aggregati dei clienti, nel contesto di più articolati *cluster* di utenza che consentono il passaggio da un modello di analisi statico, incentrato sui servizi e prodotti telefonici offerti, ad un modello più dinamico volto a comprendere ed a valorizzare le nuove esigenze della clientela. In entrambi i provvedimenti sono state previste specifiche misure di sicurezza rispetto al trattamento dei dati aggregati della clientela ai fini della composizione dei *cluster* di utenti, nonché specifiche prescrizioni rispetto all'informativa da rilasciare agli stessi ai sensi dell'art. 13 del Codice, alle moda-

11

lità per consentire l'opposizione degli interessati, in tutto o in parte, al trattamento dei propri dati in maniera celere ed agevole, nonché alla conservazione dei dati ed alla loro successiva cancellazione, ovvero anonimizzazione (provv.ti 15 ottobre 2015, n. 534, doc. web n. 4541143 e 17 dicembre 2015, n. 663, doc. web n. 4698620).

Carte fedeltà

In relazione all'attività di profilazione e *marketing*, in particolare nel settore delle carte fedeltà, sono state sottoposte all'Autorità, anche ai sensi del provvedimento generale 24 febbraio 2005 (doc. web n. 1103045), alcune istanze di verifica preliminare. Una è stata presentata da parte di una società promotrice di un programma di fidelizzazione basato sulla raccolta dei dari personali di frequentarori di sale bingo detentori di carte fedelrà. Con l'istanza in questione è stato chiesto al Garante di valutare il possibile rilascio di un'autorizzazione in merito alla conservazione dei dati personali dei clienti per finalità di profilazione e *marketing* per un periodo superiore ai 12 e 24 mesi fissati nel richiamato provvedimento generale, indicato dalla società in cinque anni.

L'Autorirà, considerate le particolati caratteristiche degli interessati fruitori dei servizi resi, i quali più agevolmente che in altri settori possono essere distinti in frequentatori abituali ovvero occasionali delle sale bingo, ha provveduto ad un accoglimento parziale della richiesta a seguito di un bilanciamento degli interessi dei soggetti coinvolti. Ha pertanto reputato congruo un periodo massimo di conservazione dei dati utilizzati dalla società titolare per attività di profilazione della clientela pari a 12 mesi, con l'aggiunta di un ulteriore periodo non superiore a tre mesi per consentire l'eventuale monitoraggio e la profilazione effettuata in relazione a eventi annualmente ricorrenti. Ha poi consentito, alla società di beneficiare di modalità di cancellazione dei dati che non necessitino di un aggiornamento con cadenza quotidiana, certamente più onerose, ma che possano essere effettuate anche per periodi e dunque a blocchi, purché non superiori ad un trimestre.

Con riguardo ai successivi trattamenti effettuati pet finalità di *marketing*, è stato infine ritenuto congruo autorizzare la conservazione dei relativi dati per un periodo non superiore a 24 mesi (provv. 2 luglio 2015, n. 394, non pubblicaro ai sensi dell'art. 24 reg. Gatante 1° agosto 2013).

All'Autorità è stata presentata, inoltre, un'istanza di verifica preliminare da parte di una società promotrice di un noto programma di fidelizzazione ai fini dell'autorizzazione a conservare i dati dei clienti, detentori della carta fedeltà, per finalità di profilazione e *marketing* per un periodo superiore a quello fissato nel menzionato provvedimento generale. L'istanza ha in particolare riguardato la possibilità di utilizzare, a fini di profilazione aggregata, i dati delle operazioni effettuate da detentori della carta che non avessero fornito il consenso alla profilazione individuale, nonché la possibilità di ottenere, dai soggetti interessati, un consenso unico per le attività di profilazione e di correlato *marketing* mirato.

L'Autorità, ha stimato congruo un periodo massimo di conservazione dei dati utilizzati dall'istante per attività di profilazione individuale e *marketing* della clientela di 24 mesi e, per attività di profilazione aggregata, di 36 mesi, disponendo che, alla relativa scadenza, i dati vengano cancellati in modo automatico e non reversibile. Ha inoltre disposto specifiche e stringenti misure giuridiche e tecniche per garantire il corretto trattamento dei dati dei detentori della carta fedeltà per finalità di profilazione aggregata (nello specifico analisi di macro fenomeni relativi a *trend* generalizzati di consumo rispetto a determinate categorie merceologiche) senza l'acquisizione dello specifico consenso degli stessi, in forza di un bilanciamento di interessi operato ai sensi del cit. art. 24 del Codice. Il Garante ha invece escluso la possibilità di ricorrere all'acquisizione di un consenso unico per finalità di profilazione

e correlato *marketing* mirato, richiamando il chiaro disposto dell'art. 23 del Codice ed esteso anche a tali ambiti le previste misure di sicurezza, oltre che disposto altri accorgimenti avuto riguardo al modello di informativa da rendere agli interessati, ai sistemi ed alle banche dati utilizzati dalla società, nonché al trasferimento dei dati all'estero (provv. 15 gennaio 2015, n.17, non pubblicato ai sensi dell'art. 24 reg. Garante 1° agosto 2013).

Media

Il Garante si è pronunciato su due istanze di *prior checking* presentate da società operanti nel settore dei *media* nell'ambito del medesimo gruppo, sempre rispetto al trattamento di dati personali degli utenti per finalità di profilazione e *marketing*.

La prima istanza si riferiva alla raccolta in forma aggregata ed al monitoraggio di dati di visione generati dai telespettatori nell'ambito di un servizio che consente di rivedere i programmi televisivi riferibili alla programmazione settimanale di alcune specifiche reti televisive, fruibili in digitale terrestre o via internet attraverso l'utilizzo di dispositivi *set-top box* o *smart* tv, su cui vengono scaricate le applicazioni.

La seconda istanza si riferiva all'analisi aggregata di informazioni relative alla visione di appositi canali *tv pay* e *free* sia della società istante, sia generalisti, attraverso televisori e *decoder* (associati ad un numero di *smartcard*) predisposti per una connessione alla rete internet. In entrambi i casi i trattamenti erano rivolti all'analisi delle prestazioni del servizio per migliorare l'offerta rendendola più aderente ai gusti del pubblico televisivo e i dispositivi utilizzati erano caratterizzati dalla presenza di un codice identificativo univoco, sottoposto ad apposite tecniche di *hashing*, al fine di non consentirne l'intellegibilità. In considetazione di tale circostanza l'Autorità, dopo una complessa attività istruttoria, ha avuto modo di precisare che i processi di cifratura applicati a tali codici consentivano comunque di mantenere una univocità di corrispondenza tra dato originario e dato cifrato e che pertanto era possibile, individuando i dispositivi ad essi associati, risalire anche indirettamenre all'utente televisivo.

Conseguentemente, entrambe le società hanno integrato i propri sistemi tecnici e previsto l'utilizzo dei dati dei telespettatori e dei codici identificativi dei dispositivi dopo aver acquisito il consenso preventivo degli stessi. Nel quadro delineato l'Autorità ha pertanto previsto, in entrambi i provvedimenti l'adozione di una serie di misure relative al corretto rilascio dell'informativa agli utenti, alle modalità concrete di esercizio dei diritti di cui all'art. 7 del Codice ed in particolare del diritto di revoca del consenso rilasciato dal telespettatore, nonché alla conservazione dei dati (provv.ti 12 marzo 2015, n. 144, doc. web n. 3881392 e 23 aprile 2015, n. 241, doc. web n. 4015426).

Alta moda

Il Garante ha adottato un provvedimento prescrittivo a seguito di un'istanza di verifica preliminare presentata da una società di alta moda, al fine di profilare la propria clientela per offrire servizi specifici ed effetruare attività promozionali personalizzate (cd. *marketing* profilato) mediante la conservazione e il trattamento dei dati personali dei propri clienti per un periodo superiore a quello previsto di 12 e 24 mesi (cfr. cit. provv. generale 24 febbraio 2005). Si ricorda che già negli ultimi anni il Garante aveva adottato provvedimenti simili riguardanti il medesimo settore (provv.ti 30 maggio 2013, n. 263, doc. web n. 2547834; 7 novembre 2013, n. 500, doc. web n. 2920245 e 24 aprile 2013, n. 219, doc. web n. 2499354). Nella richiesta pervenuta, la società ha prospettato un tempo di conservazione dei dati personali pari a dieci anni. Il Garante (ricordando che tali attività necessitano, comunque, del consenso degli interessati) ha titenuto di prescrivere come congruo un periodo di conservazione di sette anni (analogamente a quanto stabilito nei due cit. provv.ti del 2013), in relazione sia alle finalità prospettate, sia alla tipologia di dati personali oggetto di trattamento. Inoltre, ha reputato i menzionati termini di con-

servazione adeguati ai rischi degli interessati, in quanto trattandosi di beni di cd. "fascia alta", i cui acquisti vengono effettuati di massima una o due volte l'anno, un periodo inferiore di conservazione avrebbe reso, di fatto, inutile la profilazione. Il Garante, dunque, ha impartito specifiche e puntuali prescrizioni alla società che, quindi, potrà effettuare attività di profilazione e *marketing* profilato solamente previo consenso specifico dell'interessato e adottando ulteriori misure quali apposite procedure di autenticazione ed autorizzazione, obbligarorierà del tracciamento dei *log* di accesso a ciascun sistema informatico per sei mesi (in modo da realizzare un controllo analitico *ex post* delle attività svolte dai singoli incaricati). Peraltro, la società potrà conservare i dati personali della propria clientela solo per il periodo individuato nel provvedimento (sette anni), al termine del quale dovrà provvedere alla cancellazione automatica dei dati, ovvero alla loro permanente trasformazione in forma anonima (provv. 2 dicembre 2015, n. 632, doc. web n. 4642844).

11.5. *Il* mobile ticketing

Come riferito nella Relazione 2014 (cfr. p. 96), in merito ai nuovi servizi di pagamento attraverso il telefono cellulare, il Garante ha adottato un provvedimento generale sul *mobile remote payment* (provv. 22 maggio 2014, n. 258, doc. web n. 3161560), riservandosi di intervenire con ulteriori provvedimenti anche nel settore dell'offerta e dei pagamenti di titoli digitalizzati per l'accesso a servizi di utilità sociale o in mobilità. In tal senso, tenuto conto del quadro normativo vigente (in particolare d.l. n. 179 del 18.10.2012, cd. "Decreto sviluppo-*bis*", convertito con modificazioni nella l. n. 221 del 17.12.2012, della l. n. 147 del 27.12.2013, anche in considerazione della successiva l. n. 124 del 07.08.2015), dopo aver svolto un'attività conoscitiva in tali ambiti, ha avviato, con provvedimento 10 settembre 2015, n. 467 (doc. web n. 4273074), una pubblica consultazione su uno schema di provvedimento generale in materia di trattamento dei dati personali nell'ambito dei servizi di *mobile ticketing* che prevede una serie di tutele per garantire agli interessati che vogliano acquistare, via sms, biglietti dell'autobus o dei parcheggi o fruire con tale modalità di servizi di *car sharing* o *bike sharing*, oppure accedere ad aree a traffico limitato. Ciò, nell'ottica di fornire un quadro organico di regole rivolte a tutti i soggetti coinvolti, come i soggetti che offrono servizi per la mobilità e il trasporto nelle aree urbane ed extraurbane, i nuovi operatori di matrice non bancaria come gli operatori di telecomunicazioni, gli *hub* tecnologici che forniscono la piattaforma tecnologica per la distribuzione ed il pagamento dei *ticket* digitali, nonché i soggetti che gestiscono circuiti di intermediazione e gli operatori bancari, laddove l'operazione di pagamento preveda la registrazione ad un apposito sito web, nonché la titolarità di uno strumento di pagamento tradizionale come la carta di credito.

11.6. *Il contrasto allo* spam

Nel corso dell'anno sono state numerose le segnalazioni riguardanti la ricezione di comunicazioni indesiderate con modalità automatizzate, in particolare tramite *e-mail*, e, in misura decisamente minore, tramite sms e fax. L'Autorità ha proseguito nell'attività di contrasto allo *spam*, analizzando i casi segnalati e avviando varie istruttorie con riferimento ai trattamenti oggetto di segnalazioni più numerose oppure con profili di maggiore criticità, come invio di comunicazioni indesiderate

anche dopo l'opposizione al trattamento e/o la difficoltà degli interessati nell'esercizio dei diritti di cui agli artt. 7 ss. del Codice.

In molti casi, è risultato difficile individuare i titolari del trattamento, sia per le modalità con cui si può operare in rete, sia perché talora i siti mittenti risultano intestati a soggetti fantasiosi o comunque privi di recapiti utilmente contattabili, sia perché spesso essi hanno sede in Paesi (anche extraeuropei), ove l'Autorità non ha competenza (v. art. 5 del Codice).

Al riguardo, va però ribadito che l'attività di contrasto al fenomeno dello *spam* proveniente dall'estero incontra ancora ostacoli a causa di alcune differenze tra le legislazioni degli Stati europei, non solo in termini di disciplina sostanziale ma anche per quanto attiene alle tutele azionabili, con particolare riferimento alla tipologia di soggetti tutelati dagli ordinamenti in questo specifico ambito (persona fisica, persona giuridica, enti, associazioni ...). Differenze che, si auspica, verranno eliminate o comunque attenuate con l'entrata in vigore e l'implementazione del nuovo regolamento UE in materia di protezione dei dati personali, almeno riguardo a profili essenziali quali i soggetti aventi diritto alle tutele previste dalla normativa in materia di prorezione dei dati, i diritti tutelabili presso le Autorità nazionali preposte, i criteri di raccordo fra le competenze di tali Autorità (qualora si tratti di trattamenti di dati che interessino più ordinamenti nazionali) (cfr. par. 22.3).

Si segnalano, in materia, i provvedimenti 18 novembre 2015, n. 605 (doc. web n. 4487559) e 13 maggio 2015, n. 291 (doc. web n. 4337465) relativi alla modifica della formula di acquisizione del consensi per la finalità di *marketing* in sede di raccolta dei dati, quale attività spesso propedeutica all'invio di comunicazioni promozionali indesiderate e quindi alla produzione di *spam* (cfr. par. 11.3).

11.6.1. Trattamento per finalità promozionali di dati personali estratti dal database *della* mobile number portability

A seguito di numerose segnalazioni ricevute in merito ad sms promozionali che indicavano nel testo il gestore di appartenenza del ricevente, il Garante ha avviato un'istruttoria per verificare le modalità con cui era stato posto in essere tale trattamento.

Ne è emerso che la socierà che aveva curato la realizzazione della campagna promozionale si era avvalsa, essendo regolarmente iscritta al Registro operatori di comunicazione (Roc), del *database* della *mobile number portability* per individuare il gestore di appartenenza di ogni destinatario e personalizzare così maggiormente il messaggio promozionale. Il Garante pertanto ha dichiarato illecito tale trattamento in quanto le finalità di tale banca dati sono chiaramente definite dalla specifica disciplina dell'Agcom, che l'ha istituita, ed escludono espressamente l'utilizzo della stessa per finalità promozionali (provv. 23 luglio 2015, n. 436, doc. web n. 4260977).

11.7. *Le notificazioni di* data breach

Sono pervenute all'Autorità 49 comunicazioni di *data breach*, formulate dai più importanti fornitori di servizi di comunicazione elettronica operanti in Italia, registrando una crescita più che raddoppiata rispetto all'anno precedente.

La maggior parte delle violazioni notificate ha riguardato l'accesso non autorizzato ai dati personali o la perdita accidentale di documentazione contrattuale.

Inoltre, la quasi totalità dei casi notificati ha riguardato eventi che hanno coinvolto un numero di interessati inferiore a 100 essendosi verificati solo in 4 casi *data breach* di portata più ampia (oltre 2.000 soggetti coinvolti).

In tutti i casi sinora esaminati, l'Autorità, all'esito delle istruttorie svolte nei confronti dei fornitori, ha verificato che erano state adottate misure idonee a porre rimedio alle violazioni subite e a prevenirne di analoghe assicurandosi, al contempo, che gli interessati erano stati informati dagli operatori nei casi previsti. Tuttavia, in un paio di casi si è reso necessario invitare gli operatori ad effettuare in maniera tempestiva la comunicazione agli interessati ritenendo che, contrariamente alle valutazioni fatte dall'operatore, ne ricorressero i presupposti (note 17 aprile e 22 dicembre 2015).

In quattro casi, è stato avviato un separato procedimento sanzionatorio per mancato rispetto dei termini previsti per la notificazione; in un caso infatti l'operatore aveva notificato l'evento al Garante e agli interessati con sei mesi di ritardo, mentre negli altri tre casi gli operatori non avevano effettuato alcuna comunicazione, ma il Garante è staro comunque informaro degli eventi attraverso segnalazioni pervenute da soggetti interessati dalle violazioni.

L'Autorità ha inoltre affrontato questioni di portata internazionale che in alcuni casi hanno avuto una vasta eco sui mezzi d'informazione (si veda, ad es., il caso Ashley Madison), interagendo con le competenti autorità estere per verificare l'eventuale e corretto trattamento dei dati personali di cittadini italiani.

Accanto alla gestione ordinaria delle comunicazioni di *data breach*, il Garante ha esaminato gli approfondimenti svolti in materia a livello europeo, partecipando ad una serie di incontri con le altre autorità competenti in ambito comunitario. I remi di maggiore rilievo hanno riguardato le modalità concrete da adottare in caso di violazioni di dati personali a carattere transnazionale e la valurazione delle misure tecnologiche di protezione adottate dai fornitori, con particolare riferimento all'inintelligibilità dei dati.

11.8. Data retention

È proseguira l'artività ispettiva avviata a partire dal 2012 in collaborazione con il Nucleo speciale *privacy* della Guardia di finanza nei confronti di fornitori di servizi di comunicazione elettronica accessibili al pubblico. Tali accertamenti sono volti a verificare il rispetto delle prescrizioni del Codice e del provvedimento generale del Garante in mareria di conservazione dei dati di traffico telefonico e telematico (provv. 17 gennaio 2008, doc. web n. 1482111, modificato dal provv. 24 luglio 2008, doc. web n. 1538224).

In diversi casi sono state accertate e contestate violazioni amministrative relativamente alla conservazione dei dati di traffico oltre i termini previsti e alla mancata adozione di alcune delle ulteriori misure di protezione prescritte dal cit. provvedimento del Garante, quali l'uso di tecnologie di riconoscimento biometrico per selezionare l'accesso alle aree e ai sisremi dove sono conservati i dati. In nessun caso, tuttavia, si è reso necessario adottare un provvedimento in quanto gli operatori hanno adottato tempestivamente idonee misure correttive.

11.9. *La geolocalizzazione di* smartphone *di persone disperse*

Il Garante ha dato parere favorevole all'uso di nuove tecnologie volte alla geolocalizzazione di persone disperse in montagna, capaci di rendere più rapide ed efficienti le operazioni di soccorso. I due nuovi sistemi, sottoposti al vaglio dell'Autorità dal Corpo nazionale soccorso alpino e speleologico (Cnsas), trasmetteranno i dati di

geolocalizzazione dello *smartphone* dei dispersi a una centrale operativa dedicata del Cnsas, senza l'intermediazione dell'operatore telefonico e il consenso delle persone da soccorrere.

Il citato parere è stato espresso anche alla luce di quanto già stabilito nel provvedimento 19 dicembre 2008 (doc. web n. 1580543) e fatte salve alcune condizioni: che i dati raccolti dal Cnsas riguardino esclusivamente la posizione geografica del terminale della persona dispersa o infortunata e non i dari relativi al traffico o altre tipologie di dati eccedenti o non pertinenti; tali dati siano utilizzati dal Cnsas soltanto per lo scopo di salvaguardare la vita o l'integrità fisica delle persone disperse o infortunate e, pertanto, solo quando siano state attivate formalmente le ricerche di tali soggetti; i medesimi dati siano raccolti da parte del personale del Cnsas appositamente incaricato ai sensi dell'art. 30 del Codice; tali tecnologie siano attivate sull'apparecchio della persona dispersa o infortunata in modo da abilitare le funzionalità di trasmissione delle coordinate gps, ovvero l'invio di sms contenenti le coordinate delle stazioni radio base visibili dal terminale, unicamente per il tempo necessario alla localizzazione del terminale (provv. 22 gennaio 2015, n. 32, doc. web n. 3736199).

12 La protezione dei dati personali nel rapporto di lavoro pubblico e privato

Il Garante ha seguìto le importanti innovazioni della disciplina laburistica introdotte dai decreti legislativi attuativi della l. n. 183/2014 (cd. *Jobs Act*) ed in particolare la novella dell'art. 4, l. n. 300/1970 introdotta con il d.lgs. n. 151/2015, che modifica, in modo significativo, la regolazione dei controlli a distanza dei lavoratori. L'Autorità ha espresso la propria posizione nel corso dei lavori parlamentari in sede di audizioni del Presidente da parte delle Commissioni lavoro della Camera e del Senato, avvenute rispettivamente il 9 e il 14 luglio 2015 (doc. web n. 4119045).

I provvedimenti adottati dal Garante in questo ambito nel 2015 si riferiscono, peraltro, a casi rispetto ai quali trovava applicazione la disciplina previgente e confermano che, in relazione all'utilizzo di strumenti che consentono il controllo a distanza dei dipendenti, si riscontra un'area significativa di trattamenti non conformi alla disciplina sul trattamento dei dati personali.

Il Garante è altresì intervenuto in merito al trattamento di dati biometrici dei lavoratori per finalità di sicurezza, al trattamento di dati personali nella gestione del rapporto di lavoro, con particolare riguardo alla comunicazione all'esterno di dati relativi a lavoratori, alla loro pubblicazione e alle possibili interferenze con la disciplina in materia di trasparenza.

12.1. *I controlli a distanza mediante videosorveglianza*

Obbligo di informativa

In relazione all'utilizzo di sistemi di videosorveglianza nell'ambito del rapporto di lavoro, anche nel 2015 sono state accertate violazioni della disciplina applicabile in materia di protezione dei dati, in particolare dell'obbligo di informare con modalità adeguate gli interessati in ordine alle caratteristiche dei sistemi adottati nonché dell'obbligo di conformarsi a quanto prescritto dalla disciplina di settore in materia di controlli a distanza.

All'esito di accertamenti ispettivi disposti presso le sedi di una Provincia, l'Autorità ha, pertanto, dichiarato l'illiceità di un sistema di videosorveglianza in relazione al quale non si era provveduto ad apporre i prescritti cartelli informativi in prossimità del raggio di azione delle telecamere né era stata fornita adeguata informativa ai dipendenti. È emerso, inoltre, che l'ente non aveva provveduto ad attivare la procedura di garanzia prevista dall'art. 4, l. 20.5.1970, n. 300 (provv. 30 luglio 2015, n. 455, doc. web n. 4261028).

Allungamento tempi di conservazione

Il Garante ha, inoltre, esaminato alcune istanze di verifica preliminare volte ad ottenere la conservazione delle immagini raccolte attraverso sistemi di videoripresa oltre il termine massimo di sette giorni individuato in termini generali, in applicazione del principio di proporzionalità del trattamento, dal provvedimento in materia di videosorveglianza (provv. 8 aprile 2010, doc. web n. 1712680, v. punto 3.4).

In tutti i casi esaminati (quattro) l'Autorità ha riconosciuto l'esistenza, in concreto, di speciali esigenze di ulteriore conservazione da parte dei titolari del trattamento, legare a particolari esigenze di sicurezza di persone e/o di beni in relazione alle specifiche attività svolte. I soggetti richiedenti, che operano nel settore della produzione farmaceutica, dell'esazione dei pedaggi autostradali e dell'organizzazione e

gestione di manifestazioni fieristiche di beni di valore, hanno prospettato termini di conservazione ritenuti nel complesso congrui (rispettivamente 60, 20 e 10 giorni).

Del tutto peculiare è stata l'istanza di verifica preliminare presentata dalla Banca d'Italia in relazione all'attività di produzione, confezionamento e distruzione di banconote euro e di carta filigranata, posto che le relative condizioni di sicurezza (compresi i termini di conservazione per 12 mesi delle immagini raccolte) sono disciplinate da puntuali decisioni della Banca centrale europea, dotate di efficacia vincolante nei confronti dell'istituto di emissione.

Il Garante ha, altresì, ritenuto conformi al principio di proporzionalità le concrete modalità dei prospettati trattamenti, all'esito di una valutazione che ha riguardato, ad esempio, la limitazione dell'angolo di ripresa delle telecamere o l'indicazione di limiti all'accessibilità delle immagini conservate. In proposito si segnala anche che, in relazione all'attività di esazione dei pedaggi, la società richiedente si è impegnata ad adottare specifiche cautele, affinché pure i dipendenti di soggetti terzi che effettuano servizi di vigilanza siano preventivamente ed adeguatamente informati circa le caratteristiche del sistema di videosorveglianza installato.

In tutti i casi, infine, l'Autorità ha verificato che fosse stata rispettata la disciplina di settore applicabile in materia di controlli a distanza dei dipendenti (provv.ti 8 gennaio 2015, n. 4, non pubblicato ai sensi dell'art. 24 del reg. Garante 1° agosto; 12 marzo 2015, n. 142, doc. web n. 3822691; 8 luglio 2015, n. 413, doc. web n. 4253008; 17 settembre 2015, n. 476, doc. web n. 4360913).

Videosorveglianza "mobile"

Sistemi di videosorveglianza sono utilizzati, sempre più di frequente, da Forze di polizia locale nell'ambito del perseguimento delle funzioni istituzionali individuate dall'ordinamento.

In relazione a tale fenomeno il Garante, in un caso particolare, ha ritenuto illeciti i trattamenti di dati personali effettuati da un consorzio di polizia locale sia attraverso l'adozione di un sistema di videosorveglianza "mobile" operante sul territorio dei comuni aderenti al consorzio - con l'installazione sulle macchine di servizio di telecamere collocate in modo da riprendere la parte anteriore del veicolo, la carreggiata e il marciapiedi - sia mediante la localizzazione geografica dei palmari forniti in dotazione agli agenti in servizio.

L'Autorità ha, in primo luogo, ritenuto interamente applicabile la disciplina posta dal Codice, in considerazione della necessaria unicità dell'attività di videosorveglianza svolta in concreto, seppure preordinata alla effettuazione di una pluralità di trattamenti. Tale valutazione è stata effettuata con riguardo ad alcuni specifici trattamenti svolti dal consorzio – in materia di "monitoraggio del traffico" e di "vigilanza sull'integrità e sulla conservazione del patrimonio pubblico e dell'ambiente" non rientranti nell'ambito di applicazione dell'art. 53 del Codice (che dispone una disciplina parzialmente derogatoria in caso di attività svolta da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione accertamento o repressione dei reati purché prevista da espressa disposizione di legge).

Con riferimento a tale sistema è stata riscontrata l'omessa attivazione della procedura di garanzia prevista dalla disciplina in materia di controlli a distanza sull'attività dei lavoratori (v. artt. 114 del Codice e 4, l. 20.5.1970, n. 300) e la mancata informativa ai diversi soggetti interessati in ordine alle caratteristiche del sistema di videosorveglianza, e – nel dichiarare illecito il trattamento effettuato (e successivamente interrotto) – l'Autorità ha ritenuto che il consorzio, in caso di riattivazione del sistema, dovrà non solo rendere un'idonea informativa ai dipendenti ma anche individuare specifiche modalità per rendere nota alla cittadinanza l'attivazione di tale particolare modalità di sorveglianza (ad es., apponendo idonea cartellonistica e

inserendo informazioni in proposito all'interno dei siti istituzionali dei comuni interessati e del consorzio).

Per quanto riguarda la specifica funzionalità di localizzazione geografica applicata ai dispositivi mobili (palmari) consegnati ai dipendenti, è stato disposto il divieto del trattamento (ancora in atto) sia per l'omessa notificazione al Garante (dovuta ai sensi dell'art. 37 del Codice), sia – anche in questo caso – per la mancata attivazione della procedura di garanzia in materia di controlli a distanza, sia – infine – in considerazione di alcune concrete modalità del trattamento effettuato ritenute eccedenti rispetto alle finalità perseguite (provv. 8 gennaio 2015, n. 2, doc. web n. 3723437).

12.2. *I controlli sull'utilizzo di posta elettronica aziendale e di internet*

Internet

L'utilizzo dei sistemi di comunicazione elettronica (ad es., la posta elettronica aziendale) e internet, – già oggetto, in termini generali, del provv. 1° marzo 2007, n. 13, Linee guida per posta elettronica e internet, doc. web n. 1387522 –, è stato esaminato, in particolare con riguardo al trattamento dei dati personali riferiti alla navigazione internet dei dipendenti, a seguito di accertamenti ispettivi effettuati presso una società operante nel settore dei servizi di comunicazione e promozione commerciale. All'esito dell'accertamento l'Autorità ha dichiarato illecito il trattamento effettuato in violazione degli artt. 11, comma 1, lett. *a*), 13, 114 del Codice, nonché dell'art. 4, l. n. 300/1970, nel testo originario, con la conseguente inutilizzabilità dei dati trattati in violazione di legge, ai sensi dell'art. 11, comma 2, del Codice e disposto il divieto dell'ulteriore trattamento su base individuale dei dati personali riferiti alla navigazione internet dei dipendenti, con conservazione di quelli comunque trattati ai fini della eventuale acquisizione da parte dell'autorità giudiziaria (5 febbraio 2015, n. 65, doc. web n. 3813428).

Oltre, infatti, all'assenza di un'informativa completa circa le effettive caratteristiche del sistema, nonché di una *policy* volta a disciplinare in modo puntuale l'utilizzo degli strumenti elettronici affidati in dotazione ai lavoratori, il sistema era stato configurato con funzionalità tali da permettere la memorizzazione sistematica dell'indirizzo di dettaglio delle singole pagine web (cd. url) richieste e visitate dagli utenti (dipendenti e collaboratori della società), consentendo un controllo della navigazione web individualmente effettuata da soggetti identificabili. Il sistema consentiva, ad es., di generare *report* su base individuale per il tramite dell'amministratore di sistema e di estrapolare i dati di dettaglio relativi alla risorsa internet visitata (url), all'IP sorgente e all'orario di connessione, in presenza di un collegamento univoco tra i dati relativi alla connessione e la persona utilizzatrice, consentendo, quindi, di ricostruirne l'attività (cfr., par. 4 Linee guida cit.; nonché, provv. 21 luglio 2011, n. 308, doc. web n. 1829641, confermata da Trib. Roma, sez. I, 21 marzo 2013 n. 4766; cfr. anche provv.ti 2 aprile 2009, doc. web n. 1606053 e 1° aprile 2010 doc. web n. 1717799).

Trattamenti effettuati sull'*account* di posta elettronica di *ex* dipendenti

Nel solco di un orientamento già espresso con le citate Linee guida per posta elettronica e internet, l'Autorità ha ribadito che il datore di lavoro, in occasione della effettuazione di controlli sul corretto utilizzo di strumenti forniti in dotazione ai dipendenti nell'ambito del rapporto di lavoro, deve in ogni caso salvaguardare la libertà e la dignità dei lavoratori. Inoltre, conformemente ai principi di liceità e correttezza, deve fornire un'informativa chiara e dettagliata in ordine alle consentite modalità di utilizzo degli strumenti aziendali e l'indicazione puntuale delle tipologie di eventuali controlli che possono essere effettuati anche su base individuale. È

stato, pertanto, ritenuto illecito, e conseguentemente vietato, il trattamento effettuato da una società mediante la raccolta e la successiva produzione in giudizio di alcune *e-mail* (con indicazione sia dei dati cd. esterni che del loro contenuto) scambiate tra determinati dipendenti e tra questi e terze persone, senza aver previamente adottato un disciplinare o strumento analogo sull'utilizzo della posta elettronica aziendale e senza aver fornito una specifica informativa ai dipendenti. Il Garante ha, altresì, ritenuto che la società, nel trattare per finalità ulteriori – effettuazione di controlli per dichiarati scopi di tutela del patrimonio aziendale – dati raccolti al diverso fine di consentire la continuità e l'efficienza dei sistemi aziendali, abbia violato il principio di finalità dei trattamenti effettuati (v. art. 11, comma 1, lett. *b*), del Codice).

In conformità ai princìpi in materia di protezione dei dati personali, in caso di cessazione del rapporto di lavoro gli *account* riconducibili a persone identificate o identificabili devono essere disattivati, adottando contestualmente sistemi automatici volti ad informare i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento. Non è invece conforme ai suesposti princìpi reindirizzare automaticamente su indirizzi di posta elettronica aziendale i messaggi in transito su *account* attribuiti ad *ex* dipendenti (provv. 30 luglio 2015, n. 456, doc. web n. 4298277).

12.3. *Il trattamento di dati personali nella gestione del rapporto di lavoro*

La comunicazione e la diffusione dei dati personali riferiti ai dipendenti

L'Autorità continua a ricevere segnalazioni e reclami relativi a forme di conoscibilità di informazioni personali riferite al personale oppure alle modalità di circolazione delle stesse all'interno delle amministrazioni. In particolare, oggetto di verifica sono state le comunicazioni, tramite inoltro di una *e-mail* al personale docente e non docente di un Ateneo, nonché la successiva diffusione, tramite pubblicazione sul sito istituzionale dell'Università, di un documento che conteneva dati personali riguardanti emolumenti erogati in favore di alcuni dipendenti nominativamente indicati; il documento dava conto di presunte irregolarità nella gestione delle risorse economiche. Premesso che il datore di lavoro pubblico può trattare i dati personali dei lavoratori nei limiti in cui ciò sia necessario per la corretta gestione del rapporto di lavoro (cfr. le indicazioni già fornite in via generale con le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, adottate con provv. del 14 giugno 2007, n. 161, doc. web n. 1417809), il Garante ha ritenuto, sulla scorta di precedenti in materia che – impregiudicati i profili in ordine alla regolarità sul piano contabile delle erogazioni effettuate –, il personale destinatario della comunicazione elettronica non aveva titolo alcuno per venire a conoscenza dei dati in questione relativi ai colleghi (artt. 3 e 11, comma 1, lett. *d*), del Codice). Sarebbe stato quindi rispettoso del diritto alla dignità, riservatezza e alla protezione dei dati di ciascuno degli interessati provvedere a comunicazioni individualizzate. È stato pertanto dichiarato illecito il trattamento dei dati personali per effetto delle modalità comunicative utilizzate (inoltro a tutto il personale dell'Ateneo di una *e-mail* recante in allegato il cit. documento) per violazione degli artt. 11, comma 1, lett. *a*) e 19, comma 3, del Codice, vietandone l'ulteriore eventuale comunicazione (cfr. già provv. 2 marzo 2011, n. 89, doc. web n. 1802433 e, sul punto, provv. 20 dicembre 2012, n. 431, doc. web n. 2288474 e provv. 18 luglio 2013, n. 358, doc. web n. 2578201, che, con riguardo a specifici casi, hanno confermato le cit. Linee guida, in particolare, punto 5.2). Con la stessa decisione è stata altresì dichiarata illecita la diffusione di dati personali,

contenuti nel medesimo documento, in quanto effettuata in assenza di idonea base normativa (artt. 11, comma 1, lett. *a*) e 19, comma 3, del Codice) ed è stato vietato al titolare del trattamento l'ulteriore diffusione in internet, tramite il sito web istituzionale, dei dati personali riferiti al personale. La pubblicazione del documento all'interno della sezione amministrazione trasparente del siro web dell'Ateneo, infatti, è stata ritenuta illecita, stante la mancata previsione dell'obbligo di pubblicazione di tale tipologia di dati personali tra quelle puntualmente disciplinate dal legislatore nell'ambito del quadro normativo in materia di trasparenza (in particolare, il d.lgs. 14 marzo 2013, n. 33), né, pertanto è stato ritenuto applicabile, come invece sostenuto dall'Universirà, il regime di conoscibilità stabilito dalla normativa sulla trasparenza e in particolare la previsione concernente l'arco remporale quinquennale di permanenza sul web (di cui all'art. 8, comma 3, d.lgs. n. 33/2013; sul punto, cfr. introduzione, parte I, punto I e parte II, provvedimento generale n. 243, 15 maggio 2014, doc. web n. 3134436, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effertuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati) (provv. 30 luglio 2015, n. 457, doc. web n. 4278610).

12.4. *La pubblicità e trasparenza dei dati dei lavoratori*

In più occasioni il Garante è stato chiamato a pronunciarsi sulla pubblicazione *online* sui siti istituzionali degli enti pubblici ovvero nell'ambito delle sezioni dedicate all'albo pretorio, di dari, atti o provvedimenti contenenti dati personali riferiti a lavoratori - già oggetto di precedenti pronunce e da ultimo con le citate Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicirà e trasparenza sul web da soggetti pubblici e da altri enti obbligati - accertando in molti casi l'illiceità del trattamento per violazione della disciplina di settore (ad es., con riguardo alla mancata osservanza dei termini massimi di pubblicazione) ovvero per mancata osservanza del principio di pertinenza e non eccedenza dei dati pubblicati rispetto alle spesso invocate finalità di adempimento agli obblighi dettati in materia di pubblicità e trasparenza degli atti amministrativi.

In parricolare, a fronte della lamentata pubblicazione di una delibera sul sito web di una Regione, che conteneva valutazioni sulla professionalità e sul contegno di un dipendente e con la quale si disponeva il trasferimento ad altro ufficio, è stata riscontrata l'illiceità della diffusione di tale atto in assenza di idonea base normativa, non potendo a tal fine essere invocata la specifica previsione concernente l'arco temporale quinquennale di permanenza sul web stabilito dalla disciplina in materia di ttasparenza (art. 8, comma 3, d.lgs. n. 33/2013), stante la mancata previsione dell'obbligo di pubblicazione di tale tipologia di atti tra le ipotesi puntualmenre elencate dal legislatore nel capo II del citato decreto o in altra specifica norma in materia di trasparenza. Queste norme – ha ricordato il Garante – prevedono obblighi di pubblicazione nella apposita sezione del sito istituzionale denominata "Amministrazione trasparente" di informazioni "concernenti l'organizzazione e l'attività delle pubbliche amministrazioni" per favorire forme diffuse di controllo sul perseguimento delle funzioni e sull'utilizzo delle risorse pubbliche (artt. 1, comma 1 e 2, comma 2, d.lgs. n. 33/2013) e vanno mantenute distinte, anche sotto il profilo del diverso regime giuridico applicabile, dalle specifiche disposizioni di settore che regolano altri obblighi di pubblicità degli atti amministrativi per finalità diverse dalla trasparenza (cfr. introduzione, parte I, punto I e parte II, Linee guida cit.). Nel

ricordare che l'adempimento ad un obbligo di pubblicazione *online* di informazioni e documenti contenenti dati personali deve avvenire in ogni caso nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato (art. 2 del Codice), l'illiceità della diffusione è stata altresì rilevata anche alla luce del principio di pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice), atteso che la delibera riportava le valutazioni in merito all'operato del dipendente nell'esecuzione della propria prestazione lavorativa e le specifiche ragioni poste a fondamento del trasferimento ad altro ufficio (provv. 26 marzo 2015, n. 182, doc. web n. 3882453).

12.5. *La pubblicazione* online *di dati idonei a rivelare la condizione di disabilità*

Il Garante è stato nuovamente chiamato a pronunciarsi sulla pubblicazione da parte di soggetti pubblici di graduatorie concorsuali o altri atti immediatamente visibili in rete tramite i più diffusi motori di ricerca generalisti e contenenti in chiaro i dati identificativi riferiti a centinaia di soggetti in condizione di invalidità o disabilità (provv. 24 settembre 2015, n. 489, doc. web n. 4281191). In questo ambito, al fine di sensibilizzare regioni ed enti locali al rispetto della disciplina in materia di protezione dei dati personali, il Presidente dell'Autorità ha inviato due note, indirizzate rispettivamente al Presidente della Conferenza delle regioni e delle province autonome e al Presidente dell'Unione delle province italiane (note 25 settembre, doc. web n. 4281218 e 26 novembre 2015), anche a seguito di alcuni interventi che hanno portato il Garante a dichiarare l'illiceità della diffusione di dati sulla salute dei soggetti interessati (art. 22, comma 8, del Codice) – sovente unitamente ad altre informazioni eccedenti (ad es., in un caso, il codice fiscale degli stessi) – e a disporre il divieto dell'ulteriore diffusione in internet, con la prescrizione ai titolari del trattamento (enti pubblici, aziende sanitarie locali, province e regioni) dell'adozione di idonei accorgimenti nelle operazioni di trattamento funzionali alla pubblicazione di tali atti e attivazione dei conseguenti procedimenti sanzionatori sul piano amministrativo (cfr., anche, le cit. Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, parte II, punti 1 e 3.*b*).

12.6. *I quesiti in materia di trasparenza*

Nel fornire riscontro a specifiche richieste di parere o quesiti formulati dalle pp.aa. e altri soggetti istituzionali, con riguardo all'applicazione della normativa in materia di protezione dei dati nell'ambito dell'osservanza degli obblighi di pubblicazione obbligatoria stabiliti dalla normativa in materia di trasparenza, il Garante ha esaminato una richiesta avente ad oggetto la compatibilità con il quadro giuridico in materia di protezione dei dati personali di una proposta emendativa di norme regolamentari di un Comune. Al fine di dare effettività alle norme in materia di anticorruzione, l'ente locale richiedente intendeva introdurre con proprio regolamento un obbligo di pubblicazione sul web di dati patrimoniali dei dirigenti con incarico a tempo determinato, dei consulenti e collaboratori. Nel prendere atto che il legislatore delegato, nell'esercizio della propria competenza legislativa esclusiva (art. 117, comma 2, lett. *m*), Cost. e art. 1, comma 3, d.lgs. n. 33/2013), ha delimitato le categorie dei soggetti con riguardo ai quali devono essere pubblicate *online* le informazioni relative allo stato patrimoniale degli interessati, il Garante ha preci-

sato che l'eventuale estensione al personale dirigenziale con regolamento comunale degli obblighi di cui all'art. 14, d.lgs. 14 marzo 2013, n. 33 si porrebbe in contrasto con il quadro normativo in materia di protezione dei dati non potendo tale norma - che disciplina, in particolare, gli obblighi di pubblicazione dei dati reddituali e patrimoniali dei soli componenti degli organi di indirizzo politico e dei loro familiari - costituire idonea base normativa per la lecita diffusione delle stesse informazioni riferite anche alla dirigenza pubblica (artt. 4, comma 1, lett. *m*), 11, comma 1, lett. *a*) e 19, comma 3, del Codice). Ai titolari di incarichi dirigenziali e di collaborazione e consulenza trova invece applicazione l'art. 15, d.lgs. n. 33/2013 che prevede la pubblicazione obbligatoria del compenso complessivo percepito dai singoli soggetti interessati, non invece, come detto, la pubblicazione di informazioni relative alle dichiarazioni dei redditi di costoro e dei loro familiari, ipotesi questa che la legge impone esclusivamente nei confronti dei componenti degli organi di indirizzo politico (cfr., punti 9.b. e 9.c, parte I, Linee guida, cit.). Nel sollecitare un bilanciamento fra i valori costituzionali in gioco e il rispetto della normativa comunitaria in materia di protezione dei dati personali sia in fase interpretativa del diritto vigente che in sede di esercizio del potere normativo (cfr. art. 6, par. 1, letr. *c*), e art. 7, par.1, lett. *c*) e *d*), direttiva 95/46/CE; artt. 3 e 11 del Codice; v. inoltre, CGUE, 20/5/2003, cause riunite C-465/00, C-138/01 e C-139/01), il Garante ha ribadito che, più in generale, gli enti locali e le pp.aa. non possono introdurre nuovi obblighi di pubblicazione per finalità di trasparenza con propri atti regolamentari rispetto a quanto già disciplinato dal legislatore, circostanza che potrebbe comportare un'irragionevole differenziazione non solo del livello di trasparenza ma anche, per l'effetto, di quello di protezione dei dari personali sul territorio nazionale a seconda dell'area geografica su cui insistono le competenze istituzionali dell'amministrazione presso cui opera l'interessato ovvero in base al criterio di residenza del cittadino-utente (cfr. già, parere del Garante su uno schema di decreto legislativo concernente il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pp.aa. del 7 febbraio 2013, n. 49, doc. web n. 2243168) (provv. 25 giugno 2015, n. 377, doc. web n. 4166711).

Con altro quesito è stato richiesto al Garante di formulare un proprio avviso con riguardo alla legittimità della pubblicazione, nella sezione Amministrazione trasparente di un Consiglio regionale, dei nominativi del personale con contratto a tempo determinato in servizio presso le segreterie di supporto ai gruppi politici con indicazione espressa del relativo gruppo di assegnazione. Nel premettere che l'informazione in ordine al gruppo politico in favore del quale si presta collaborazione può, in alcuni casi, rivelare le "opinioni politiche" e, in determinate circostanze, essere indicativo dell'eventuale "adesione a partiti [...o ad] associazioni [...] a carattere [...] politico" (art. 4, comma 1, lett. *d*) ed *m*), del Codice), il Garante ha precisato che in base al quadro di garanzie particolarmente stringente a tutela dei dati sensibili, i soggetti pubblici possono diffondere tali informazioni solo nel caso in cui sia previsto da una espressa disposizione di legge e, pur in presenza di puntuali obblighi di pubblicazione, solo nel caso in cui la diffusione di tali informazioni sia in concreto indispensabile in vista della finalità di rilevante interesse pubblico perseguita (artt. 11, comma 1, lett. *a*) e *d*), 20, 21 e 22, commi 3 e 11, del Codice, ma cfr. anche, art. 4, comma 4, d.lgs. n. 33/2013). Alla luce del quadro normativo (con particolare riferimento agli artt. 16 e 17, d.lgs. n. 33/2013 che mirano a dare evidenza della "dotazione organica" e del "costo del personale"), solo per il personale di diretta collaborazione con gli organi di indirizzo politico che sia, in pari tempo, titolare di un contratto a tempo determinato è prevista la pubblicazione di uno specifico "dato personale" (secondo la definizione del Codice art. 4, comma 1, lett. *b*),

del Codice), quale è il nominativo. Il Garante ha, quindi, concluso che la Regione poteva disporre la pubblicazione nella sezione Amministrazione trasparente del sito web del Consiglio regionale dei soli dati personali espressamente previsti dalla legge, ossia i nominativi del personale a tempo determinato, senza specificare, per coloro che svolgano servizio presso le segreterie di supporto ai gruppi politici, il relativo gruppo politico di assegnazione (v. art. 1, comma 2, nonché, artt. 4, 6, 8 comma 3, d.lgs. n. 33/2013; art. 8, par. 1, direttiva 95/46/CE, nonché WP Art. 29, *Advice paper on special categories of data (sensitive data)*, 4 aprile 2011) (provv. 25 giugno 2015, n. 376, doc. web n. 4699444).

12.7. *La comunicazione tra soggetti pubblici di dati relativi ai lavoratori*

Il Garante si è altresì pronunciato con riguardo alle istanze formulate ai sensi degli artt. 19, comma 2, e 39 del Codice. In particolare, il Comando di polizia locale di un Comune aveva rappresentato la necessità di ottenere l'autorizzazione a comunicare alla Regione di competenza alcuni dati personali riferiti agli operatori di polizia locale al fine di consentire la realizzazione di tessere di riconoscimento per il personale di polizia locale operante nel tetritorio tegionale. Tanto, in base al quadro normativo di riferimento e in attuazione di un apposito accordo tra la Regione stessa ed i Comuni interessati. Il Garante ha ritenuto che la fornitura di tessere di riconoscimento per il personale di polizia locale potesse essere inquadrata nell'ambito delle funzioni istituzionali di coordinamento, sostegno e supporto tecnico e finanziario in favore degli enti locali e dovesse essere considerata nell'ambito della tealizzazione di progetti per la sicurezza urbana, nonché di sostegno all'attività operativa della polizia locale; ciò, sia con riguardo alla disciplina quadro in materia di ordinamento di polizia locale (cfr. art. 6, comma 2, l. 7 marzo 1986, n. 65) che alla vigente disciplina regionale di settore. Considerata la mancanza di un'espressa previsione di legge o di regolamento che in via diretta preveda la comunicazione di dati personali degli addetti al servizio di polizia locale da parte dei Corpi operanti presso i singoli Comuni a favore della Regione, il Garante, ai sensi degli artt. 19, comma 2, e 39, comma 2, del Codice, ha stabilito che i Corpi di polizia locale presso i Comuni interessati, possono lecitamente comunicare alla Regione i pertinenti dati personali (art. 11, comma 1, lett. *d*), del Codice) riferiti al personale addetto al servizio di polizia locale e che la Regione può, a propria volta, anche per il tramite di soggetti designati responsabili del trattamento, procedere allo svolgimento delle attività di trattamento necessarie alla predisposizione e gestione delle tessere di riconoscimento, nel rispetto dei princìpi di necessità pertinenza e non eccedenza, anche sotto il profilo dei tempi di conservazione (artt. 3, 11, comma 1, lett. *b*) ed *e*), del Codice) nonché delle disposizioni che stabiliscono le misure di sicurezza (artt. 31, 33 e 34 del Codice) (provv. 28 maggio 2015, n. 317, doc. web n. 4169391).

13 Le attività economiche

13.1. *Il settore bancario*

Anche nel 2015 sono pervenute numerose segnalazioni e reclami riguardanti problematiche sulle quali il Garante ha già avuto modo di pronunciarsi con le Linee guida adottate il 25 ottobre 2007 in materia di trattamenti di dati personali effettuati da banche nei rapporti con la clientela (doc. web n. 1457247). Le istanze hanno riguardato, in particolare, i profili dell'accesso ai dati relativi a rapporti bancari (in specie di conto corrente e depositi titoli) di persone decedute, quello della richiesta di copia di documentazione riferita a rapporti bancari e quello della comunicazione a terzi di dati inerenti a clienti.

Il flusso costante di segnalazioni in questo ambito appare legato soprattutto all'attuale situazione di profonda crisi economica che, determinando l'aumento delle posizioni bancarie di temporanea difficoltà o di "sofferenza", moltiplica inevitabilmente il contenzioso banche/clientela e aumenta la necessità di ricostruire la "storia" dei rapporti contrattuali, specie con riguardo agli interessi praticati. Negli ultimi mesi, poi, appare evidente l'attenzione di numerosi correntisti degli istituti di credito interessati dalle recenti vicende di ristrutturazione o dissesto, vicende che hanno portato con sé l'esigenza dei risparmiatori di verificare la completezza e la "trasparenza" delle informazioni ricevute dagli istituti di credito.

Circolazione delle informazioni e tracciamento delle operazioni bancarie

Con riferimento ai più volte segnalati casi di illecita comunicazione di dati a terzi non legittimati, è proseguita l'attività di monitoraggio dell'adempimento da parte delle banche alle misure (sia necessarie che opportune) prescritte dal Garante all'intero settore creditizio con il provvedimento generale – adottato il 12 maggio 2011 e divenuto pienamente efficace il 1° ottobre 2014 – recante Prescrizioni in mareria di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (provv. n. 192, doc. web n. 1813953).

In tale ambito, il Garante ha deliberato di indirizzare parte dell'attività ispettiva di iniziativa curata dall'Ufficio alla verifica dell'implementazione delle prescrizioni contenute nella decisione, al fine di valutare gli effetti prodotti da un provvedimento di sicuro rilievo nella configurazione del rapporto banca/clientela, specie in riferimento alla sentita necessità di innalzare il livello di protezione dei dati personali dei clienti.

Nel corso dell'anno, pertanto, sono state effettuate diverse ispezioni nei confronti di istituti di credito, individuati a campione anche in relazione alle diverse tipologie dimensionali e operative. L'attività ispettiva proseguirà anche nel primo semestre del 2016, con l'obiettivo di fornire agli operatori coinvolti, ove all'esito dei controlli effettuati se ne dovesse ravvisare la necessità, ulteriori indicazioni, anche operative, di carattere generale.

13.2. *La revisione del codice deontologico Sic*

La grande attenzione al tratramento dei dati in ambito bancario e finanziario ha da molti anni spinto l'Autorità a confronrarsi con il correlato tema delle grandi banche dati che, già previste dal legislatore o costituite per iniziativa degli operatori del set-

tore, svolgono la delicata funzione di condividere dati e informazioni sulla situazione economica di persone fisiche e imprese al fine di indirizzare le decisioni sulla concessione del credito, attenuando il relativo rischio. Dalla più antica centrale dei rischi della Banca d'Italia ai sistemi di informazione creditizia gestiti da soggetti privati, sottoposti ad un codice di deontologia varato nell'ormai lontano 2004, sono numerosi gli strumenti di questo tipo quotidianamente consultati dagli operatori del settore. Si tratta di strumenti ormai connaturati al funzionamento del sistema creditizio e inseriti in un panorama nel quale operano anche la centrale d'allarme interbancaria e le società che forniscono servizi di informazione commerciale, realtà che parimenti sono spesso destinatarie di istanze di esercizio dei diritti di cui all'art. 7 del Codice.

In questo quadro economico e normativo, sono proseguiti i lavori volti alla revisione del cd. codice deontologico Sic, a dieci anni dalla sua entrata in vigore.

L'Autorità ha ultimato la verifica dei requisiti di partecipazione al tavolo di lavoro prescritti dal provvedimento 17 aprile 2014, n. 203 (doc. web n. 3070048) – nel rispetto del principio di rappresentatività di cui all'art. 2, comma 2, reg. n. 2/2006 del Garante sulle procedure per la sottoscrizione dei codici di deontologia e di buona condotta – in capo ai soggetti interessati a prendervi parte e ha formalizzato l'esclusione di quelli privi dei requisiti richiesti, comunicando, invece, l'avvio dei lavori a quelli ammessi a parteciparvi.

Nel corso di specifici incontri, sono state individuate le tematiche da approfondire in sede di revisione del codice e la metodologia da seguire, costituendo a tal fine un tavolo tecnico ristretto composto, tra gli altri, da rappresentanti dei gestori dei Sic, degli istituti di credito e delle società finanziarie (i cd. partecipanti) e delle associazioni dei consumatori e deputato a proporre le modifiche da apportare al codice e, in generale, ad interagire con l'Autorità per garantire un più agevole e spedito svolgimento dei lavori.

Alcuni dei partecipanti ai lavori hanno sollevato, in via preliminare, il problema del ruolo da attribuire ai nuovi soggetti che "possono avere accesso" ai Sic ai sensi dell'art. 6-*bis*, d.l. 13 agosto 2011, n. 138 (inserito dalla l. di conversione 14 settembre 2011, n. 148, per effetto del rinvio all'art. 30-*ter*, d.lgs. 13 agosto 2010, n. 141), avuto riguardo, in particolare, ai fornitori di servizi di comunicazione elettronica e alle imprese di assicurazione.

La questione sollevata, da definire nel corso del 2016 e propedeutica al prosieguo dei lavori, mira, nelle intenzioni dei proponenti, a prevedere che tali "nuovi" soggetti contribuiscano nei cd. Sic anche i dati relativi ad interessati privi di una storia creditizia, in modo da diventare "partecipanti pieni" (come definiti dall'art. 1, comma 1, lett. *e*) del codice deontologico) ai sistemi di informazioni creditizie conformemente al principio di reciprocità che ha finora presieduto alla costituzione di questo tipo di banche dati.

13.3. *Il fenomeno delle morosità nel settore delle cd.* utilities

Costituzione di una banca dati relativa a morosità intenzionali nel settore telefonico (S.I.Mo.I.Tel.)

Il rilievo e le potenzialità espresse nell'ambito economico-finanziario dalle diverse centrali rischi cui si è fatto cenno nei paragrafi precedenti, hanno innescato da alcuni anni la spinta (prima a livello di riflessione nell'ambito delle categorie economiche e professionali, poi anche a livello di progettazione normativa) a riprodurre questo modello anche in ambiti molto diversi da quelli da cui storicamente ha tratto origine. Poiché, a tutt'oggi, manca un organico quadro normativo (di cui peraltro si avverte sempre di più la necessità), il Garante si è trovato (e si trova) nella necessità di esaminare, sulla base dei princìpi generali del Codice e della normativa comuni-

taria per i profili di interesse, i diversi progetti che al riguardo vengono, con sempre maggiore frequenza, proposti. Da questo punto di vista, l'anno 2015 ha costituito una tappa significativa; primo banco di prova è stato rappresentato dal settore delle telecomunicazioni.

L'8 ottobre 2015, al termine di un intenso confronto che ha accompagnato e seguito la consultazione pubblica relativa allo schema di provvedimento già adottato dall'Autorità con delibera n. 154 del 27 marzo 2014 e relativo al progetto di costituzione del cd. SIT (provv. n. 523, doc. web n. 3041680), è stato adottato un ptovvedimento che prevede la costituzione di una banca dati relativa a morosità intenzionali della clientela del settore telefonico (doc. web n. 4349760). A seguito di numerose riserve sollevate soprattutto dalle associazioni dei consumatori e di profili problematici rappresentati anche dal Consiglio nazionale dei consumatori e degli utenti presso il Ministero dello sviluppo economico, l'Autorità ha svolto numerosi incontri con i rappresentanti degli operatori telefonici e con un'ampia rappresentanza di associazioni di consumatori. L'attività di dialogo e confronto e l'ampio coinvolgimento di realtà associative ha portato all'elaborazione di proposte operative in larga parte condivise tra le parti e poi recepite nel provvedimento. La banca dati di cui si è prevista la costituzione è radicalmente diversa da quella inizialmente ipotizzata, non essendo più assimilabile a una centrale rischi negativa di settore, ma piuttosto ad un sistema che censirà solo coloro (persone fisiche e giuridiche, enti, associazioni, titolari di ditte individuali e liberi professionisti) che non paghino intenzionalmente le bollette telefoniche relative a pacchetti comprensivi di abbonamento e fornitura di *smartphone* o *tablet*, con esclusione, invece, dei soggetti che si rendano eventualmente e temporaneamente inadempienti ai propri obblighi contrattuali perché inesperti, distratti o interessati da momentanee difficoltà economiche. Obiettivo del provvedimento è dunque quello di contrastare il fenomeno del cd. "turismo telefonico", costituito da utenti che passano da un operatore all'altro lasciando intenzionalmente bollette insolute pur avendo acquisito la disponibilità di un dispositivo spesso di significativo valore economico. Da qui l'individuazione della nuova denominazione di Sistema informativo sulle morosità intenzionali nel settore della telefonia (S.I.Mo.I.Tel.), che sottende una profonda differenza dello strumento e delle sue finalità rispetto a quello originariamente ipotizzato.

Lo scambio di informazioni sulle morosità intenzionali tra gli operatori telefonici (partecipanti alla banca dati) può quindi risultare uno strumento utile per valutare e contenere condotte destinate ad incidere non solo sui bilanci degli operatori, ma anche su altri utenti incolpevoli e in regola con i pagamenti, i quali potrebbero essere costretti a sopportare costi altrimenti non dovuti. Nel Sistema – consultabile dagli operatori prima dell'attivazione di un nuovo contratto e gestito da un soggetto che verrà individuato dagli stessi operatori telefonici, presumibilmente entro l'anno 2016 – potranno essere trattate solo informazioni riguardanti i mancati pagamenti del cliente ad esclusione, in particolare, di dati sensibili e giudiziari. Le informazioni sulle morosità potranno essere inserite nel S.I.Mo.I.Tel. solo in presenza di specifici requisiti: recesso dal contratto da non meno di tre mesi; morosità superiore a 150 euro per singolo operatore; fatture non pagate nei primi sei mesi successivi alla stipula del contratto; assenza di altri contratti tutt'ora attivi con lo stesso operatore. Prima di essere inserito nel sistema il cliente dovrà essere avvertito dall'operatore telefonico dell'imminente iscrizione. Le informazioni sui pagamenti non regolarizzati saranno conservate per 36 mesi e poi verranno cancellate automaticamente. I dati raccolti non potranno essere usati per altre finalità (ricerche di mercato, pubblicità, *marketing*). In applicazione dell'istituto del bilanciamento di interessi, previsto dall'art. 24, d.lgs. n. 196/2003, l'Autorità ha ritenuto che il trattamento dei

dati contenuti nel S.I.Mo.I.Tel. possa essere effettuato dal gestore del Sistema e dagli operatori telefonici senza consenso degli interessati, purché sia preceduto da un'informativa chiara e puntuale da rendere in occasione della stipula del contratto. Allo scopo di gestire la fase di avvio del sistema, si è anche previsto che, entro 60 giorni dalla pubblicazione del provvedimento in Gazzetta Ufficiale, gli operatori rendano anche un'informativa preventiva all'ampia platea di clienti i cui rapporti sono già in essere e che potrebbero essere censiti nella banca dati. Una volta che gli operatori telefonici avranno individuato il soggetto privato cui affidare la gestione del Sistema, dovranno comunicare al Garante il nome e la sede della banca dati, ed almeno tre mesi prima dell'entrata in funzione, dovranno inviare copia dell'accordo sottoscritto dalle parti per consentire all'Autorità di valutarne la conformità alle prescrizioni dettate. Al gestore spetta invece l'obbligo di notificare al Garante il trattamento dei dati prima del suo inizio.

La collaborazione con l'Autorità per l'energia elettrica e il gas

L'Autorità ha reso all'Autorità per l'energia elettrica ed il gas la richiesta collaborazione per valutare la correttezza del trattamento dei dati personali della clientela derivante da specifici interventi ipotizzati da Aeeg e volti a contrastare, nel breve periodo, la rilevante crescita del fenomeno della morosità nel mercato di riferimento.

In particolare, sono state fornite talune indicazioni affinché il trattamento da parte del nuovo venditore (di energia elettrica e gas) di dati personali ulteriori (rispetto a quelli contenuti nei contratti) dei clienti interessati alla procedura di cd. *switching* – già puntualmente regolamentata con disposizioni di rango primario e secondario – sia anche conforme al Codice. I chiarimenti resi mirano a consentire una più precisa e completa valutazione delle condizioni in cui avverrà la futura fornitura e permettere, eventualmente, di rinunciare al cambio richiesto revocando il contratto concluso prima della sua esecuzione (nota 8 maggio 2015, doc. web n. 4702076).

13.4. *Il nuovo codice di deontologia e di buona condotta in materia di informazioni commerciali*

L'attenzione al tema delle grandi banche dati ha portato anche alla definizione delle regole di deontologia per il trattamento dati in un settore, quello delle informazioni commerciali, che pur essendo storicamente consolidato, si è mosso per lunghi anni in un ambito estremamente povero di riferimenti normativi. Al termine di un'istruttoria lunga e complessa, durata circa cinque anni, con il provvedimento 17 settembre 2015, n. 479 (doc. web n. 4298343) è stato adottato il codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato ai fini di informazione commerciale (v. art. 118 del Codice) destinato a tutti i soggetti che si trovino o vogliano operare nel settore relativo alle attività di informazione commerciale sul territorio italiano (ai sensi dell'art. 134, r.d. n. 773/1931, e successive modificazioni ed integrazioni, recante il t.u. delle leggi di pubblica sicurezza e relativi regolamenti di attuazione). In particolare, non solo viene sancito che l'attività di raccolta delle informazioni debba avvenire nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, e segnatamente del diritto alla protezione dei dati personali, del diritto alla riservatezza e del diritto all'identità personale (art. 2 del Codice), ma vengono, altresì individuate, nel rispetto dei princìpi sanciti dall'art. 11 del Codice, adeguate garanzie e modalità di trattamento dei dati personali che mirino a garantire la qualità, la pertinenza, l'esattezza e l'aggiornamento dei dati personali trattati. Profilo questo di particolare rilievo in quanto, nella corrente attività d'impresa, le decisioni quotidianamente assunte in sede di contrattazione fra diversi sog-

getti economici e ancor più le decisioni in materia di finanziamento vengono assunte proprio sulla base dei *report* informativi e delle valutazioni espresse dagli operatori della cd. informazione commerciale. Naturalmente, il codice deontologico si applica alle sole informazioni commerciali riferite a persone fisiche (rientranti nel concetto di interessato di cui all'art. 4, comma 1, lettera *i*), del Codice) ed, in particolare, al trattamento dei dari personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque o pubblicamente accessibili da chiunque, nonché al trattamento avente ad oggetto i dati personali forniti direttamente dagli interessati, effettuato dai soggetti che prestano a terzi servizi, per finalità di informazione commerciale, nel rispetto dei limiti e delle modalità che le normative vigenti stabiliscono per la conoscibilità, utilizzabilità e pubblicità di tali dati; resta, pertanto, esclusa la sua applicazione alle informazioni commerciali riferite alle persone giuridiche. Il codice, infine, detta regole più semplici sia relativamente all'informativa, sia relativamente all'esercizio dei diritti dell'interessato. Particolarmente significativa e oggetto di un'elaborazione attenta e prudente, è la disciplina concernente la possibilità di trattare informazioni tratte da fonti giornalistiche sia cartacee che *online* (di cui all'art. 3, comma 2, del codice di deontologia). È un'apertura verso un modello di informazione commerciale più completo e circostanziato, ma anche più esposto a rischi di inesattezza o comunque suscettibile di costante aggiornamento. Ne è specifica testimonianza anche la disposizione sul trattamento dei dati giudiziari (di cui al comma 5 del cit. art. 3). Non meno rilevante è, poi, il complesso di disposizioni che (specie nell'art. 7) mirano a delimitare il perimetro dei soggetti censibili e soprattutto l'eventuale collegamento degli stessi con le realtà imprenditoriali e societarie nelle quali hanno operato o rispetto alle quali hanno esercitato ruoli o nelle quali sono stati titolari di posizioni volta a volta ritenute significative e rilevanti.

13.5. *Il settore assicurativo*

In ambito assicurativo, l'Autorità è stata più volte chiamata a esprimere il proprio parere in merito ad alcuni atti regolamentari o provvedimentali adottati dall'Ivass. Ciò, con riferimento particolare a quel complesso di banche dati di recente costituzione, implementate essenzialmente per consentire una più efficace attività antifrode nel settore della responsabilità civile automobilistica.

Con riferimento alla banca dati degli attestati di rischio (art. 134, comma 2, d.lgs. n. 209/2005), il Garante, nell'esprimere parere sul regolamento Ivass n. 9 del 19 maggio 2015, sul collegato provvedimento n. 35 del 19 giugno 2015 e sui relativi allegati tecnici (provv. 30 luglio 2015, n. 454, doc. web n. 4252652), ha richiamato l'Istituto sulla necessità di perfezionare i testi sottoposti ad esame, sia per quanto riguarda la specificazione del ruolo delle imprese in fase di alimentazione e consultazione della banca dati, delle finalità sottese alla trasmissione delle informazioni e delle misure di sicurezza da garantire a protezione di queste ultime (regolamento), sia per quel che concerne il richiamo al rispetto della disciplina del Codice e ai diritti degli interessati, il rilascio di alcune opportune indicazioni in tema di informativa e consenso, la previsione di un termine massimo di conservazione delle informazioni. Non sono risultati problematici, invece, altri profili regolarori concernenti, in particolare, la proporzionalità del trattamento e la qualità dei dati.

Su altro versante, il Garante è stato poi chiamato a valutare talune modifiche che l'Ivass avrebbe voluto apportare, sulla base di alcuni interventi normativi anche recenti e delle osservazioni pervenute all'esito della pubblica consultazione, al "nuovo" schema di regolamento recante la disciplina della banca dati sinistri, della banca dati anagrafe

testimoni e della banca dati anagrafe danneggiati (art. 120 del Codice; art. 135, d.lgs. n. 209/2005). L'Autorità ha ricordato, tra l'altro, la necessità di rispettare i principi di finalità e proporzionalità, circoscrivendo l'accesso alle informazioni contenute nelle predette banche di dati ai soli soggetti legittimati in base alla legge, oltre che in rapporto alle finalità "antifrode" sottese alla loro istituzione (art. 11, comma 1, lett. *b*) e *d*), del Codice). Inoltre, è stata chiarita la necessità di modificare il testo nella parte relativa alla nozione di "interessati", non più comprensiva dei soggetti riconducibili a persone giuridiche, enti o associazioni (art. 40, d.l. 6 dicembre 2011, n. 201, convertito con modificazioni dalla l. 22 dicembre 2011, n. 214).

13.6. *La videosorveglianza in ambito privato*

Nel corso dell'anno, è proseguito l'afflusso di segnalazioni e reclami concernenti le più svariate ipotesi di installazione di videocamere. La tipologia di istanze proposte conferma l'elevato livello di contenzioso sia con riguardo alle installazioni per finalità esclusivamente personali (art. 5, comma 3, del Codice) sia con riguardo a quelle in ambito condominiale.

La base di riferimento è ovviamente costituita dal provvedimento generale dell'8 aprile 2010 (doc. web n. 1712680) in ordine al quale l'Ufficio ha avviato un lavoro di revisione e aggiornamento tenendo conto anche delle novità tecnologiche che moltiplicano la possibilità di effettuare videoriprese (basti pensare all'utilizzo di droni o alla diffusione delle cd. *dash cam*).

Per ciò che riguarda, invece, le istanze di verifica preliminare sottoposte al Garante, vale rilevare che tutte hanno riguardato la richiesta di allungare i tempi di conservazione delle immagini registrate dai sistemi di videosorveglianza oltre i sette giorni al fine di rafforzare il livello di sicurezza del sito oggetto di videosorveglianza.

In particolare, si è trattato di aziende che operano nel campo della produzione di beni anche di lusso e dei trasporti intermodali di merci. Tutte le richieste hanno avuto un esito favorevole e sono state valutate tenendo in considerazione, non solamente i parametri di sicurezza previsti dalle normative internazionali, comunitarie e nazionali, ma le acclarate difficoltà delle società di accertare, in tempi più contenuti, eventuali illeciti verificatisi. Ciò in relazione alle tempistiche connesse alla verifica delle giacenze o a quelle relative alle spedizioni internazionali.

13.7. *Il recupero crediti*

È un'attività che dà luogo ad un trattamento dati spesso molto invasivo e, per le concrete modalità del suo svolgersi, difficilmente monitorabile, rispetto al quale, quindi, è più difficile individuare comportamenti illeciti. Con riferimento ad un trattamento "tracciabile" il Garante, con provvedimento del 28 maggio 2015, n. 319 (doc. web n. 4131145), a seguito della segnalazione di un abbonato di Sky Italia s.r.l., si è pronunciato su un sistema che la società aveva predisposto per recuperare importi insoluti dovuti dai propri clienti. Il sistema prevedeva l'invio, al *decoder* del cliente, di messaggi di sollecito visualizzabili sullo schermo del televisore sotto forma di *banner* contenenti l'icona di una busta: il tasto del telecomando che consentiva la lettura del messaggio, oppure la chiusura del *banner* per leggere il messaggio in un secondo momento, poteva essere azionato senza limitazioni da chiunque si trovasse davanti allo schermo; ne conseguiva la possibilità che terzi estranei conoscessero la posizione debitoria dell'abbonato (peraltro contestata in concreto dal segnalante). Il Garante,

richiamando anche le ptescrizioni già rese in passato in materia di trattamenti di dati personali effettuati nell'esercizio di attività di recupero in sede stragiudiziale di crediti (v. provv. generale 30 novembre 2005, doc. web n. 1213644), ha stabilito che tale trattamento di dati non fosse lecito, tenuto conto che, per le modalità utilizzate, lo stato di insolvenza degli abbonati si prestava ad essere conosciuto da un numero indeterminato di soggetti; ha pertanto prescritto a Sky Italia s.r.l., qualora inrendesse continuare ad utilizzare il sistema dei messaggi sul televisore anche per finalità di recupero crediti, di adottare specifiche misure volte ad escludere il rischio, anche potenziale, di diffusione a terzi di informazioni sulla situazione debitoria dei propri abbonati. In particolare la società avrebbe dovuto prevedere l'utilizzo di un codice di accesso al contenuto del messaggio da consegnare a qualunque cliente al momento della sottosctizione del contratto e da utilizzare per leggere il messaggio, ferma restando la necessità di privilegiare, in ogni caso, per l'invio di solleciti di pagamento altre modalità, quali ad esempio la comunicazione via *e-mail* o l'invio di una comunicazione all'indirizzo del cliente. La società ha successivamente comunicato al Garante di essersi adeguata alle prescrizioni contenute nel provvedimento e di averne dato notizia alla clientela con apposito comunicato stampa.

13.8. *Altre attività imprenditoriali*

Autonoleggio ed *event data recorder*

Come nel 2013 (v. provv. 7 novembre 2013, n. 499, doc. web n. 2911484), l'Autorità è stata chiamata a valutare la liceità dei trattamenti connessi all'installazione, a bordo del parco veicoli in dotazione a una società di autonoleggio, di dispositivi satellitari multifunzione annoverabili tra i cd. *event data recorder*. Tali dispositivi, in grado di raccogliere e trasmettere ad appositi fornitori di servizi numerose informazioni relative alle singole vetture (e indirettamente, ai relativi conducenti), sarebbero stati utilizzati dalla società per garantire alcuni servizi (gestione di eventuali sinistri; ritrovamento dei veicoli rubati; assistenza stradale; monitoraggio chilometri e tempi di utilizzo; diagnostica) ai propri clienti. All'esito di una complessa attività istruttoria, l'Autorità ha ammesso i trattamenti oggetto dell'istanza, ritenendoli conformi – ove effettuati nel rispetto delle modalità indicate – ai princìpi di liceità, necessità, finalità e proporzionalità (artt. 3 e 11 del Codice); tuttavia, sono state prescritte alla società alcune misure volte ad assicurare un'effettiva tutela degli interessati, sia sul piano delle misure di sicurezza e dei requisiti che devono possedere, rispettivamente, i fornitori dei servizi descritti e i dispositivi eletttonici utilizzati (ove carenti in tal senso), oltre che il portale web accessibile dal titolare, sia sul piano della modulistica utilizzata ai fini del rilascio dell'informativa agli interessati e dell'acquisizione del relativo consenso (da emendare in funzione delle indicazioni contenute nel provvedimento adottato). Nel prescrivere, tra le altre, anche la distruzione dei dati personali non più necessari in rapporto agli scopi petseguiti nell'ambito dei singoli servizi offerti, ha poi ribadito che i dati trattati attraverso tali tipologie di sistemi non possono essere utilizzati dai titolari per finalità diverse da quelle dichiarate e, in particolare, per profilare i conducenti o negare la stipula di nuovi contratti di autonoleggio (provv. 7 maggio 2015, n. 270, doc. web n. 4167756).

Franchising

A seguito di un reclamo, l'Autorità è stata poi chiamata a valutare la liceità del trattamento effettuato da alcuni collaboratori operanti nell'interesse, tra l'altro, di un *franchisor*. La reclamante contestava l'invio (documentato in atti), da parte dei predetti collaboratori, di una *e-mail* contenente propri dati personali e sensibili ad alcuni *franchisee*, senza che tale comunicazione fosse sorretta da adeguati presupposti giustificativi. A seguito di una approfondita istruttoria – volta a chiarire, in capo

ai molteplici soggetti coinvolti (collaboratori, *franchisor*, società appaltatrici e subappaltatrici), il ruolo effettivamente svolto da ciascuno nella vicenda e le relative eventuali responsabilità – il Garante ha ritenuto, anche sulla base dei rapporti in essere tra le singole società, che i collaboratori avessero agito per finalità, nell'interesse e a tutela, anzitutto, del *franchisor* e che a tale soggetto (unitamente ad una delle società appaltatrici coinvolte, operante in piena autonomia) doveva essere ascritta la responsabilità del relativo operato. Muovendo da tali premesse, accertata l'assenza di idonei presupposti per il trattamento dei dati personali e sensibili dell'interessata, ha provveduto a dichiararne l'illiceità, vietando al *franchisor* e alla società co-titolare l'ulteriore trattamento dei medesimi dati, fatta salva la loro conservazione a fini di giustizia. Ha inoltre prescritto alle due società di adottare idonee misure atte a garantire una scrupolosa vigilanza sui soggetti incaricati di operare nel loro interesse e/o per loro conto, sensibilizzando costoro al puntuale rispetto delle istruzioni ricevute nella veste di incaricati del trattamento (art. 30 del Codice); è stato prescritto, infine, al *franchisor* di designare una delle società appaltatrici coinvolte nella vicenda quale responsabile *ex* art. 29 del Codice (provv. 23 aprile 2015, n. 242, doc. web n. 3966213).

Esonero dell'informativa

A seguito di un'avvenuta cessione di ramo di azienda, l'Autorità ha esonerato una compagnia aerea dall'obbligo di rendere l'informativa agli interessati (in particolare, ai clienti, alle altre controparti contrattuali ed i ai dipendenti della società cedente).

Al riguardo – come già sostenuto in altre occasioni - ha rilevato che in ragione della peculiare disciplina che regola la cessione di ramo di azienda (artt. 2558, 2559, 2560 e 2112 c.c.) sul piano sostanziale, si viene a determinare una successione legale del nuovo imprenditore in tutti i rapporti giuridici e in tutte le posizioni attive e passive facenti capo al cedente, sicché, subentrando l'acquirente nella stessa posizione dell'alienante, il trattamento dei dati personali connessi alla gestione dei rami di azienda ceduti, non necessita di alcun consenso, trovando applicazione il presupposto equipollente di cui all'art. 24, comma 1, lett. *b*), del Codice, che consente di prescindere da esso nel caso in cui il trattamento sia necessario per eseguire obblighi derivanti da un contratto di cui sia parte lo stesso interessato. Ciò premesso, restando comunque doveroso il rispetto dell'obbligo di informativa posto dall'art. 13 del Codice che, nell'ipotesi in cui i dati personali non siano raccolti direttamente presso l'interessato, impone al titolare del trattamento di rendere l'informativa "all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione" (comma 4), - dopo aver verificato l'impossibilità di rendere l'informativa a tutti gli interessati in forma individuale in ragione della natura sproporzionata dei mezzi astrattamente impiegabili - ha accolto la richieste di esonero, ai sensi dell'art. 13, comma 5, lett. *c*), del Codice, prescrivendo specifiche modalità alternative e semplificate (provv. 19 febbraio 2015, n. 97, doc. web n. 3864423).

14 I dati biometrici

14.1. *Il trattamento dei dati biometrici nel settore societario e professionale*

Sono pervenute al Garante numerose richieste di verifica preliminare (art. 17 del Codice) relativamente al trattamento di dati biometrici connesso all'utilizzo di soluzioni di firma di atti e documenti informatici.

In un caso, il trattamento – benché riconducibile nelle ipotesi di esonero contemplate dal provvedimento generale 12 novembre 2014, n. 513 (doc. web n. 3556992) – ha formato comunque oggetto di attenzione da parte del Garante per espressa volontà della richiedente, società ideatrice e fruitrice del sistema dalla stessa realizzato. Tale sistema, con riferimento al correlato trattamento di dati personali e biometrici, è risultato sostanzialmente conforme, sulla base delle indicazioni fornite, alle prescrizioni contenute nel richiamato provvedimento generale. L'Autorità, tuttavia, ha prescritto alla società di provvedere, se necessario, alla designazione di tutti i soggetti preposti al trattamento dei dati anche biometrici degli interessati quali incaricati *ex* art. 30 del Codice, nonché di trattare questi ultimi solo dopo aver adempiuto all'obbligo di notifica di cui agli artt. 37 e 38 dello stesso Codice (provv. 17 settembre 2015, n. 478, doc. web n. 4373152).

In un altro caso l'Autorità è stata chiamata a pronunciarsi su un trattamento connesso all'utilizzo di un sistema di firma "grafometrica" in ambito notarile. Tale sistema, preordinato alla raccolta dei dati biometrici dei partecipanti all'atto (parti, fidefacienti, interpreti, testimoni) in termini sostanzialmente conformi al menzionato provvedimento generale, non sarebbe stato riconducibile, tuttavia, alle soluzioni di firma elettronica avanzata poste a base del medesimo provvedimento generale, in ragione dei "limiti d'uso" connessi a quest'ultima (art. 60 d.P.C.M., 22 febbraio 2013). L'Autorità, nel ritenere che tale aspetto non incidesse significativamente rispetto ai sistemi in precedenza esaminati, ha ammesso il trattamento oggetto dell'istanza (proposta dal Consiglio nazionale del notariato in ragione della rilevanza per l'intera categoria professionale), prescrivendo comunque ai titolari alcune misure aggiuntive a garanzia degli interessati, tra cui l'adozione di idonei meccanismi di autenticazione "forte" per l'accesso alle postazioni e adeguati tempi di *time-out* automatico per l'applicazione utilizzata. È stata invece respinta, per altro verso, la contestuale richiesta di esonero dalla notificazione formulata ai sensi dell'art. 37, comma 2, del Codice, attesa la peculiare natura dei dati trattati e l'oggettiva rischiosità del trattamento (provv. 25 novembre 2015, n. 619, doc. web n. 4538440).

Non consta di precedenti, invece, la pronuncia in tema di riconoscimento facciale applicato a un sistema di selezione delle immagini dei passeggeri ritratti a bordo delle navi da crociera (provv. 18 giugno 2015, n. 360, doc. web n. 4170232). Tale sistema, basato sul confronto (consensuale) delle caratteristiche biometriche dei volti estratte da apposite foto-campione con quelle ricavate dagli scatti quotidianamente effettuati dal fotografo di bordo, avrebbe permesso ai passeggeri di visionare le sole immagini di propria pertinenza, evitando così accessi indistinti e generalizzati alle fotografie altrui. Inoltre, la soluzione descritta avrebbe consentito di ridurre significativamente l'impatto ambientale derivante dai processi di smaltimento dell'ingente quantitativo di fotografie invendute (pari a circa il 92%, su un totale

approssimativo di 11.300.000 scatti annuali). L'Autorità, nel valutare positivamente l'istanza presentata, ha ritenuto che il trattamento dei dati biometrici dei passeggeri, effettuato su base volontaria e secondo le modalità indicate, non fosse illecito, né sproporzionato rispetto alla finalità dichiarata; nondimeno, è stato prescritto alla società di adottare opportuni accorgimenti atti a rendere compiutamente informati gli interessati in ordine al trattamento dei loro dati anche biometrici, nonché di provvedere all'effettiva e irreversibile cancellazione, al termine del periodo di riferimento, delle foto scattate e dei codici associati ai volti ivi presenti (lecitamente trattati dal titolare per effetto del bilanciamento di interessi disposto dall'Autorità con il medesimo provvedimento). Ha inoltre raccomandato alla società di assicurare che le registrazioni degli accessi al *database* contenente i predetti codici presentassero le medesime caratteristiche di quelle richieste dal provvedimento generale sugli amministratori di sistema (provv. 27 novembre 2008, doc. web n. 1577499).

Meritano di essere citate inoltre, soprattutto per i complessi profili tecnologici esaminati, le richieste di verifica preliminare riguardanti il trattamento di dati biometrici nell'ambito di un servizio di firma digitale remota con autenticazione biometrica da parte di un istituto bancario (provv. 28 maggio 2015, n. 318, doc. web n. 4167873); il trattamento di dati biometrici nell'ambito di un sistema di firma elettronica avanzata realizzata attraverso firma grafometrica da un istituto bancario (provv. 17 dicembre 2015, n. 662, doc. web n. 4645479); il trattamento di dati biometrici connesso a una soluzione di firma elettronica avanzata basata su bio–penna (provv. 4 giugno 2015, n. 336, doc. web n. 4172308).

14.2. *Il trattamento dei dati biometrici nel rapporto di lavoro*

Con il provvedimento generale prescrittivo in tema di biometria 12 novembre 2014, n. 513 (doc. web n. 3556992) il Garante ha ribadito che il trattamento di dati biometrici, in considerazione della loro stretta (e stabile) relazione con l'individuo e la sua identità, può essere effettuato solo previa adozione di particolari cautele. In particolare, tutti coloro che intendano effettuare tale tipologia di trattamenti sono tenuti a presentare un'istanza di verifica preliminare al Garante, salvi alcuni casi di esonero puntualmente individuati, sempre che vengano adottate specifiche misure e accorgimenti tecnici e che siano rispettati i principi generali di liceità, finalità, necessità e proporzionalità dei trattamenti.

Accesso ad aree riservate

In un caso specifico l'Autorità ha ritenuto lecito il trattamento dei dati biometrici dei lavoratori (impronte digitali), prospettato da una società che gestisce spazi commerciali all'interno di alcuni aeroporti internazionali, allo scopo di consentire ai soli dipendenti previamente autorizzati l'accesso a determinate aree (ove vengono depositate merci di particolare valore o collocate particolari apparecchiature informatiche). Considerato che alla luce delle specificità del sistema prescelto non è stato ritenuto applicabile l'esonero dall'obbligo di attivazione del procedimento di verifica preliminare, con il provvedimento sono state altresì prescritte alcune cautele ritenute necessarie per rafforzare le misure di sicurezza e per tenere distinte le basi di dati relative, rispettivamente, ai riferimenti biometrici ed agli altri dati personali dei dipendenti (provv. 18 giugno 2015, n. 361, doc. web n. 4173465).

Finalità di rilevazione delle presenze

In relazione, invece, all'utilizzo di un sistema biometrico da parte di un Comune per finalità di rilevazione delle presenze in servizio dei dipendenti, all'esito di una valutazione effettuata alla luce dei principi di necessità e proporzionalità rispetto alle finalità perseguite, il Garante non ha rinvenuto ragioni specifiche in base alle quali altri e diversi strumenti automatizzati (es. il *badge*, se del caso associato ad un pin

individuale) dovessero essere ritenuti inadatti a realizzare legittimi obiettivi di efficienza nell'attività di gestione del personale, né nel caso concreto sono emersi specifici motivi per i quali il personale direttivo sarebbe srato impossibilitato a svolgere l'ordinaria attività di controllo sulla corretta esecuzione della prestazione lavorativa. Non sono, peraltro, emerse concrete ipotesi di violazione dei doveri d'ufficio da parte dei dipendenti o elementi tali da ritenere fondato il timore di abusi. È stato, altresì, rilevato che il titolare del trattamento non aveva ottemperato all'obbligo di effettuare la notificazione del ttattamento e di presentare la richiesta di verifica preliminare. Conseguentemente l'Autorità ha disposto il divieto dell'ulteriote trattamento dei dati biometrici riferiti ai dipendenti (provv. 22 ottobre 2015, n. 552, doc. web n. 4430740).

15 Attività di normazione tecnica internazionale e nazionale

Nel 2015 l'Autorità ha collaborato, armonizzando la propria posizione con quelle delle altre autorità di protezione dati per il tramite del WP29, all'elaborazione di norme tecniche nell'ambito dell'ente di standardizzazione internazionale ISO, sia all'interno del Working Group 5 - Sottocomitato 27 (SC27), competente in materia di sicurezza di gestione delle identità, biometria e *privacy*, sia e del *Joint Technical Committee* (JTC1), sulla sicurezza delle informazioni.

In particolare si menzionano:

- ISO 29134 - *Privacy Impact Assessment -Guidelines*: linea guida per condurre un *Privacy Impact Assessment* (PIA) allo scopo di valutare e mitigare i rischi relativi al trattamento di dati personali attraverso un approccio di gestione del rischio ispirato alla norma tecnica ISO 31000 e definire i controlli di sicurezza (ISO/IEC 27002) relativi alla protezione dei dati personali (ISO/IEC 29151);
- ISO 29151- *Code of practice for the protection of personally identifiable information*: catalogo di controlli per la protezione dei dati personali, sul modello dei controlli di sicurezza previsti dalla ISO/IEC 27002, nonché di controlli relativi alla protezione dei dati personali derivati dai princìpi della ISO/IEC 29100 (*Privacy Framework*).

L'Autorità, inoltre, ha contribuito ai lavori di UNINFO - l'ente di normazione federato con UNI (Ente Nazionale Italiano di Unificazione) - riguardanti:

- l'elaborazione di una metodologia basata sul sistema e-CF per definire i profili professionali di terza generazione relativi alla gestione della *privacy*;
- la revisione della traduzione italiana della ISO 29100 (*Privacy Framewok*) in cui si è tenuto conto delle definizioni presenti nella legislazione italiana e in uso corrente al momento della conclusione dei lavori (ottobre 2015);
- la stesura di una norma tecnica sui "Criteri d'identificazione delle *app* nel mondo socio-sanitario della salute" per una corretta identificazione e caratterizzazione delle *app* nonché per favorire una maggiore consapevolezza da parte degli utilizzatori.

16 Il trattamento dei dati nel condominio

In materia di condominio l'attività dell'Autorità nel 2015 è stata prevalentemente indirizzata all'analisi delle implicazioni della riforma entrata in vigore nel giugno del 2013 (l. 11 dicembre 2012, n. 220, recante modifiche alla disciplina del condominio negli edifici), al fine di fornire ulteriori chiarimenti rispetto ai profili attineuti il tema del trattamento di dati personali (cfr. Relazione annuale 2014, p. 121).

In particolare sono state nuovamente oggetto di attenzione da parte del Garante le norme inerenti le nuove "Attribuzioni dell'amministratore" relative, tra l'altro, alla tenuta di vari registri, tra i quali è ricompreso anche il cd. "registro di anagrafe condominiale" (cfr. art. 1130, comma 1, punto 6, c.c.). Al riguardo, il Garante – nel sottolineare l'alterità tra l'esercizio del diritto di accesso ai dati personali disciplinato dagli artt. 7 ss. del Codice e il diverso diritto di prendere visione e di ottenere eventualmente copia del registro nella sua interezza, ai sensi dell'art. 1129 c.c. – ha chiarito che il registro può essere visionato, previa richiesta all'amministratore, dagli interessati gratuitamente e che gli stessi possono ottenerne eventualmente copia, previo rimborso della relativa spesa. L'Autorità ha dunque colto l'occasione per ribadire, in termini generali, quanto già indicato nel provvedimento del 18 maggio 2006 in materia di trattamento di dati personali nell'ambito dell'amministrazione di condomini (doc. web n. 1297626), e cioè che la conoscibilità delle informazioni concernenti i partecipanti alla compagine condominiale deve restare impregiudicata qualora ciò sia conforme alla disciplina civilistica o comunque sia prevista in base ad altre norme presenti nell'ordinamento, purché sussistano i relativi presupposti fissati dalla legge.

In occasione di un ulteriore quesito sul tema, l'Autorità ha fatto nuovamente presente che non si ravvisa alcuno specifico obbligo a carico del condomino di allegare documenti a riprova della veridicità delle informazioni rese ai fini della costituzione del citato registro di anagrafe da parte dell'amministratore di condominio. Si è, in particolare, puntualizzato che la trasmissione all'amministratore da parte del condomino della copia autentica del titolo che determina il trasferimento del diritto di proprietà prevista dall'art. 63 disp. att. c.c. concerne, espressamente, l'ipotesi in cui viene effettuata dallo stesso un'operazione di compravendita e pertanto non riguarda propriamente la tenuta del registro dell'anagrafe condominiale da parte dell'amministratore, se non eventualmente in un'ottica di successivo aggiornamento dello stesso. La *ratio* di tale disposizione normativa, non riguarda quindi la specifica disciplina inerente la realizzazione del registro dell'anagrafe condominiale di cui all'art. 1130 c.c., ma è piuttosto volta a soddisfare l'esigenza di sollevare il proprietario dell'immobile, che cede il diritto sull'unità immobiliare a terzi, dall'obbligo di contribuzione delle spese condominiali dal momento in cui il suddetto trasferimento viene reso noto al condominio (nota 16 dicembre 2015).

17 Il trasferimento dei dati all'estero

Con riguardo al tema dei trasferimenti transfrontalieri di dati personali, l'attività del Garante si è innanzitutto concentrata, come già verificatosi in passato, sulle numerose istanze volte al rilascio di autorizzazioni al trasferimento di dati verso Paesi terzi tramite le cd. *Binding corporate rules* (Bcr). È ormai evidente il crescente interesse e il diffuso utilizzo da parte del settore privato delle Bcr quale strumento privilegiato per il trasferimento di dati personali verso Paesi terzi effettuato nell'ambito di gruppi di imprese. Stante il cospicuo numero di autorizzazioni rese nel corso degli anni, l'Autorità, nel periodo di riferimento, ha effettuato alcuni accertamenti d'ufficio volti a verificare l'effettiva adozione, nonché la corretta applicazione, da parte delle imprese facenti parte dei gruppi e operanti sul territorio nazionale, di tali strumenti di trasferimento di dati all'estero.

Per quanto concerne le istanze pervenute nel 2015 ed inerenti l'impiego delle Bcr (per lo più, aventi ad oggetto il trasferimento di dati relativi a dipendenti, clienti e fornitori), sono state avviate istruttorie complesse che si sono concluse con l'approvazione di 5 autorizzazioni rilasciate dal Garante a conclusione di un *iter* nel corso del quale è stata verificata la conformità del testo delle Bcr – approvato al termine delle procedure europee tutte di mutuo riconoscimento –, con l'ordinamento italiano e con alcuni dei principali criteri stabiliti in materia dal Gruppo Art. 29 (cfr. provv.ti 2 aprile 2015 n. 197, doc. web n. 4003088; 13 maggio 2015 n. 290, doc. web n. 4167370; 10 settembre 2015 n. 470, doc. web n. 4362580; 22 ottobre 2015 n. 551, doc. web n. 4589496; 5 novembre 2015 n. 575, doc. web n. 4587199). Tali istruttorie sono state condotte alla stregua delle verifiche poste in essere negli anni precedenti in relazione ad analoghe istanze (cfr. Relazione 2014, p. 126, con particolare riguardo ai casi, oggetto di analisi anche nel periodo di riferimento, di Bcr consistenti esclusivamente in dichiarazioni unilaterali rilasciate dalla società capogruppo o in semplici *privacy policy*).

Il 2015 – come sopra evidenziato – si è caratterizzato anche per le indagini effettuate *in loco* nei confronti di alcune società italiane operanti sia nel settore manifatturiero, sia in quello della gestione dei pagamenti alle quali, nel corso degli anni 2001-2013, il Garante ha rilasciato le autorizzazioni nazionali per consentire l'utilizzo da parte delle stesse delle Bcr.

Tali indagini hanno evidenziato, in termini generali, alcune discrasie tra quanto dichiarato dalle società italiane in sede di richiesta di autorizzazione nazionale e quanto effettivamente posto in essere dalle stesse al proprio interno. Da una parte, infatti, è emerso che alcune delle società coinvolte negli accertamenti non effettuano, in realtà, alcun trasferimento di dati personali nell'ambito del gruppo e quindi non si avvalgono, in concreto, dello strumento delle Bcr (pur richiesto ed ottenuto); dall'altra, si è potuto rilevare che in taluni casi le società, nel porre in essere i trasferimenti di dati all'estero, non sembrano avere autonomi poteri decisionali in ordine alle iniziative da intraprendere all'interno della propria struttura organizzativa per poter realizzare in concreto quanto stabilito in materia di Bcr.

L'Autorità nel verificare, nel corso dei citati accertamenti, la sussistenza o meno dei singoli requisiti previsti in materia di Bcr, ha comunque potuto rilevare alcune criticità; ciò, in particolare, con riferimento al rispetto del principio di trasparenza

17

di cui al punto 5.7. del WP 74, nonché in materia di previsione di programmi di *audit*, così come indicato al punto 5.2. del WP 74. Ha pertanto fornito, all'esito delle verifiche condotte, alcune prescrizioni alle società interessate dai controlli, invitando le stesse ad adoperarsi per assicurare a tutti gli interessati una agevole individuazione e consultazione delle Bcr ponendo, ad esempio, i documenti che le compongono in un medesimo riquadro del sito e comunque differenziandole dal contesto delle ulteriori *policy* in materia di *privacy* presenti sui siti web delle società, nonché a prevedere e realizzare al proprio interno i programmi di *audit* come indicato dal Gruppo Art. 29. A fronte di tali richieste, le società hanno provveduto a porre in essere gli opportuni accorgimenti all'interno delle proprie strutture organizzative per garantire una effettiva e corretta applicazione dei princìpi contenuti nelle Bcr che erano già state oggetto di autorizzazione.

Sotto altro profilo, l'atrenzione del Garante è stata anche rivolta all'importante novità rappresentata dalla sentenza 6 ottobre 2015 con cui la CGUE si è pronunciata in ordine alla causa C-362/14, Maximillian Schrems vs. Data Protection Commissioner, dichiarando invalida la decisione della Commissione europea 26 luglio 2000 n. 2000/520/CE con la quale era stato ritenuto adeguato il livello di protezione dei dati personali garantito dagli Stati Uniti d'America nel contesto del cd. regime di *Safe Harbor*. Considerato il forte impatto di tale pronuncia sul complesso scenario relativo ai flussi dei dati transfrontalieri che coinvolgono l'Unione europea e gli Stati Uniti d'America, la questione è divenuta oggetto di un'attenta valutazione da parte dei Garanti europei riuniti nel Gruppo Art. 29 che hanno formulato alcune preliminari osservazioni in merito agli effetti della menzionata decisione sui trasferimenti dei dati effettuati dal territorio dell'Unione europea verso gli Stati Uniti d'America e alle future iniziative che gli stessi intendono intraprendere al fine di disciplinare adeguatamente tale tipologia di flussi transfrontalieri. In tale scenario, l'Autorità è intervenuta, con riferimento all'ambito nazionale, disponendo con provvedimento 22 ottobre 2015, n. 564 (doc. web n. 4396484) la caducazione dell'autorizzazione, resa il 10 ottobre 2001 sulla base della menzionata decisione della Commissione dichiarata invalida e volta a consentire i trasferimenti di dati personali dal territorio nazionale verso organizzazioni aventi sede negli Stati Uniti e operanti nel rispetto dei princìpi del *Safe Harbor* (doc. web n. 30939).

Stante il rilievo delle novirà menzionate, anche al fine di contribuire alla menzionata attività di approfondimento attualmente in corso a livello europeo e di sensibilizzare i soggetti coinvolti da tali trasferimenti, l'Autorità ha assunto l'iniziativa di inviare alle principali associazioni di categoria operanti nel settore industriale e commerciale una richiesta di informazioni sia per comprendere la portata nazionale del fenomeno in questione sia per conoscere eventuali iniziative e misure già adottate per consentire la prosecuzione dei trasferimenti di dati nel rispetto del quadro normativo esistente (art. 44 del Codice) (cfr. par. 22.3).

18 Il registro dei trattamenti

18.1. *La notificazione*

La notificazione è una dichiarazione con la quale un titolare (sia soggetto pubblico che privato) rende nota l'effettuazione di un determinato trattamento di dati personali (specificando una serie di informazioni obbligatorie) affinché, attraverso l'inserimento nel registro dei trattamenti, tali informazioni vengano rese pubbliche. Essa è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto in ottemperanza alle istruzioni pubblicate sul sito, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione.

Le notificazioni sono inserite in un registro pubblico liberamente e gratuitamente consultabile *online* tramite il sito dell'Autorità, da cui chiunque può acquisire notizie e utilizzarle per le finalità di applicazione della disciplina in materia di protezione dei dati personali (ad es., per esercitare il diritto di accesso ai dati o gli altri diritti riconosciuti dal Codice). La notificazione del trattamento deve essere presentata al Garante prima dell'inizio del trattamento, una sola volta, indipendentemente dal numero delle operazioni e della durata del trattamento da effettuare e può anche riguardare uno o più trattamenti con finalità correlate. Una nuova notificazione è richiesta solo prima che cessi definitivamente l'attività di trattamento oppure quando si renda necessario modificare alcuno degli elementi in essa contenuti. I titolari hanno l'onere di mantenere aggiornato il registro comunicando le eventuali variazioni (quali, il cambio di sede o la denominazione della società) o la cessazione del trattamento (ad es., in occasione della cessazione dell'impresa). Nel caso in cui una pluralità di soggetti autonomi esercitano congiuntamente un potere decisionale sulle finalità e sulle modalità di un trattamento di dati personali in modo tale che si realizzi una vera e propria "contitolarità", ciascuno di essi è tenuto ad effettuare un'autonoma notificazione, nella quale indicherà anche tutti gli altri contitolari.

Le norme del Codice da tenere in considerazione quando si deve valutare la necessità di procedere a questo adempimento sono: l'art. 37 (Notificazione del trattamento) e l'art. 38 (Modalità di notificazione), per la parte sostanziale, l'art. 163 (Omessa o incompleta notificazione) e l'art. 168 (Falsità nelle dichiarazioni e notificazioni al Garante), per la parte sanzionatoria.

Occorre inoltre tenere presente che i provvedimenti di esonero dall'obbligo di notificazione o di chiarimento adottati dal Garante sono pubblicati, insieme alle istruzioni, nella sezione del sito www.garanteprivacy.it denominata "Notificazione e Registro dei trattamenti", raggiungibile dalla *home page* cliccando il *link* "servizi *online*".

18.2. *L'evoluzione della notificazione nel 2015*

Il Garante fornisce quotidianamente supporto a tutti i soggetti che notificano i trattamenti sul registro per agevolare la corretta conclusione delle procedure e chiarire eventuali dubbi sui tratramenti che necessitano di essere notificati. Al fine di ottimizzare il riscontro alle numerose richieste di chiarimenti che quotidianamente

pervengono al Garante tramite telefono o posta eletttronica, in merito alle necessità e modalità di notificazione, nonché allo scopo di agevolare il corretto e tempestivo adempimento di tale obbligo da parte dei titolari del trattamento, nel corso dell'anno è stato predisposto un documento esplicativo riportante le risposte alle domande più frequenti (cd. FAQ) finalizzato ad agevolare l'interfaccia verso l'utenza su aspetti, sia di natura tecnica che di merito, legati alla procedura di notificazione. Ad esempio, si consideri che nell'anno 2015 sono pervenute circa 1.200 richieste di chiarimento telefoniche e circa 600 tramite posta elettronica. La definitiva pubblicazione delle FAQ, oltre a fornire un servizio più celere agli utenti, consentirà, la liberazione di risorse interne da destinare ad attività più specifiche, quali, ad esempio, quelle relative ai controlli.

Nel 2015 è proseguita l'attività di controllo, sia nei confronti dei titolari iscritti nel Registro sia nei confronti di quelli che effettuano trattamenti oggetto di notificazione ma che non risultano presenti nel Registro; tale attività è stata effettuata anche mediante ispezioni *in loco*, nell'ambito della programmazione ispettiva di cui si è dato conto al par. 21.1. In particolare, dai controlli effettuati nel corso dell'anno sono emersi 44 casi di omessa o incompleta notificazione del trattamento e sono state contestate le relative violazioni ai titolari del trattamento. La maggior parte delle violazioni è stata riscontrata con riferimento al trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (art. 37, comma 1, lett. *a*) del Codice), principalmente nell'ambito del rapporto di lavoro dipendente, nel corso di un ciclo di ispezioni condotto nei confronti di alcune società di trasporti sul territorio nazionale. In rali circostanze, sono state contestate 15 violazioni per omessa notificazione ed effettuate 5 denunce in relazione alle violazioni penali riscontrate in merito agli obblighi previsti dallo Statuto dei lavoratori.

Di pari rilievo sono state le violazioni riscontrate con riferimento al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, nonché quello relativo alla prestazione di servizi sanitari per via telematica (art. 37, comma 1, lett. *b*) del Codice). Relativamente a tali trattamenti, infatti, l'Ufficio ha condotto un ciclo di ispezioni nei confronti di alcuni laboratori di analisi, dalle cui risultanze sono emerse, in particolare, 8 violazioni per l'omessa notificazione di tali trattamenti ed ulteriori 12 violazioni connesse all'incompleta norificazione; l'Ufficio ha quindi adottato i relativi atti di contestazione nei confronti dei titolari del trattamento coinvolti.

L'Ufficio ha inoltre provveduto, in ragione della numerosità delle violazioni riscontrate, ad inoltrare alle principali associazioni di categoria di rale settore, una nota volta a richiedere l'intervento delle stesse per stimolare presso i propri iscritti una verifica del corretto adempimento degli obblighi in materia di prorezione dei dati personali. In tale contesto è stato anche richiamato, quanto disposto dal Garante con il provvedimento 19 novembre 2009, recante "Linee guida in tema di referti *online*" (doc. web n. 1679033), evidenziando la necessità dell'adozione di specifiche misure di sicurezza per l'effettuazione di rale tipologia di trattamenti di dari personali. Le misure di sicurezza segnalate, difatti, appaiono necessarie al fine di prevenire possibili pregiudizi ai diritti degli assistiti, con riferimento ai trattamenti dei loro dati personali sensibili e genetici, in relazione alla fornitura di servizi di consultazione *online* dei referti o di trasmissione degli stessi per posta elerronica.

In tutti i casi sopra indicati, quindi, sono stati avviati i procedimenti per l'applicazione della sanzione prevista dall'art. 163 del Codice che prevede una pena pecuniaria da 20.000 a 120.000 euro.

Anche in ragione delle sopra esposte attività ispettive, delle numerose violazioni

contestate ai titolari e del conseguente adempimento da parte degli stessi e degli altri operatori del settore, si evidenzia che nell'anno 2015 il Registro dei trattamenti ha conseguito un picco nel numero di notificazioni pervenute. Infatti le stesse sono risultate pari a 2.622 nell'anno 2015, a fronte di una media pari a circa 1.300 notificazioni annue nell'ultimo quinquennio. Inoltre è possibile osservare come il dato relativo al 2015 sia il più elevato dell'intera serie storica delle notificazioni, fatta eccezione per l'anno 2004, anno di costituzione del Registro dei trattamenti (in cui furono effettuate più di 10.000 notificazioni) (cfr. sez. IV, tab. 12 e 14).

A tale risultato ha contribuito anche l'adozione del provvedimento generale relativo ai *cookie* (provv. 8 maggio 2014, n. 229, doc. web n. 3118884), che ha reso più evidenti ad una vasta platea di titolari gli obblighi connessi ad alcuni tipi di trattamento, come ad esempio quello relativo alla cd. profilazione degli interessati (art. 37, comma 1, lett. *d*) del Codice).

Tuttavia, anche a fronte della maggiore attenzione riscontrata rispetto a tale obbligo, occorre osservare che nella società odierna, in cui la dinamicità del trattamento dei dati passa attraverso semplici interazioni degli utenti con *app* e dispositivi interconnessi (*Internet of Things*), la staticità della notificazione appare sempre più inadeguata a garantire efficacemente i diritti degli interessati.

In questo senso quindi, nel nuovo regolamento europeo, la cui pubblicazione è prevista sulla GUUE del 4 maggio 2016, si supererà la logica della notificazione a vantaggio di nuovi strumenti più effettivi quali ad esempio l'introduzione di una nuova figura, il cd. *data protection officer* (definito nella traduzione italiana in maniera un po' infelice, Responsabile della protezione dei dati) al quale saranno affidati compiti sostanziali, per assicurare il rispetto della normativa in materia di *privacy* da parte della società o ente nell'ambito del quale viene designato. Sarà affidato a questo nuovo soggetto, dorato di una specifica professionalità nel settore della protezione dei dati personali, il ruolo di "presidio avanzato" del rispetto dei principi e degli adempimenti in materia nonché di interlocutore ed elemento di connessione tra il titolare del trattamento e l'Autorità.

19 La trattazione dei ricorsi

19.1. *I profili generali*

Il numero delle decisioni adottate nel 2015 (307) è stato pressoché uguale all'anno precedente (306) e le aree tematiche oggetto di trattazione corrispondono grosso modo a quelle sulle quali da diversi anni si concentrano la maggior parte delle questioni sottoposte al Garante in sede di ricorso.

Uno sguardo più approfondito, che tenga conto non solo del contenuto delle richieste formulate, ma anche delle ragioni sostanziali alla base dei singoli procedimenti, permette di cogliere la frequente connessione delle vicende esaminate alle varie sfaccettature della crisi economica e sociale tutt'ora in atto. Ne sono testimonianza i numerosi ricorsi nei confronti di istituti di credito e società finanziarie spesso volti ad assicurare in tempi rapidi la possibilità di ricostruire il quadro completo dei rapporti bancari riconducibili ad una persona, ad una società, o ad un defunto (art. 9, comma 3, del Codice). L'art. 7 del Codice è utilizzato come strumento per ricostruire l'assetto e l'evoluzione dei patrimoni e dei rapporti bancari personali, familiari, imprenditoriali, nonché il punto di pattenza per contestare le condizioni conrrattuali con il sistema creditizio o, più in dertaglio, per verificare la congruità dei tassi d'interesse praticati. Più spesso il diritto di accesso riconosciuto dal menzionato art. 7 costituisce lo strumento indispensabile per verificare la liceità del trattamento nell'ampio settore della centralizzazione dei rischi di credito e in quello, ancora più esteso, delle banche dati che forniscono informazioni commerciali sulle persone ovvero sulla correttezza e tempestività nell'onorare le scadenze dei pagamenti e, più in generale, sulla loro affidabilità economica. Al riguardo è importante sottolineare l'adozione da parte del Garante del codice di deontologia e buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale (provv. 17 settembre 2015, n. 479, doc. web n. 4298343), promosso dall'Autorità e redarto unitamente a vatie associazioni di categoria imprenditoriali e di consumatori e volto a regolare un settore particolarmente importante per il corretto funzionamento del mercato (cfr. par. 13.4).

Le valutazioni economiche, finanziarie e patrimoniali effettuate dalle società specializzate in questo settore infatti sono in grado di segnalare prevenrivamente eventuali rischi relativi a soggetti in affari.

Il Garante, inrervenendo nel corso degli anni, a seguito di numerosi ricorsi, aveva infatti più volte sottolineato che il non corretto utilizzo di banche dati e strumenti di analisi così invasivi può arrecare seri danni alla dignità e tiservatezza delle persone coinvolte, pertanto nel "nuovo codice" si è cercato di coniugare esigenze di semplificazione degli adempimenti cui sono tenute le società di informazioni commerciali con il diritto alla ptotezione dei dati personali dei soggetti coinvolti, e quindi di declinare al meglio quel bilanciamento fra la libertà di iniziativa economica privata e sicurezza, dignità e libertà individuale. Non è un caso, quindi, che ormai da anni il Garante sia diventato un punto di riferimento in questa matetia grazie anche agli orientamenti espressi in relazione, in particolare, all'amplissimo settore dei trattamenti svolti presso i sistemi di informazioni creditizie, la Centrale dei rischi della Banca d'Italia, la Centtale d'allarme interbancaria.

19

19.2. *I dati statistici*

Per ciò che concerne la tipologia delle decisioni, si conferma nel periodo di riferimento l'alta percentuale di decisioni di non luogo a provvedere (60%), cioè di procedimenti conclusisi con il soddisfacimento, nel corso dell'istruttoria, delle richieste degli interessati/ricorrenti. Tale dato testimonia l'utilità e l'efficacia di questa specifica forma di tutela, la cui funzione principale è quella di favorire la composizione delle controversie direttamente tra l'interessato e il titolare del trattamento. Tale obiettivo viene perseguito assicurando, da un lato, che i diritti tutelati dall'art. 7 del Codice siano esercitati con richieste mirate e chiare e dall'altro che il riscontro del titolare sia tempestivo e pertinente.

Posto che l'attivazione del ricorso dinanzi all'Autorità è passaggio necessariamente successivo rispetto alla proposizione di un apposito interpello rivolto previamente al soggetto detentore dei dati, unica eccezione, i cui limiti sono stati ben delineati dalla giurisprudenza del Garante, è costituita dal comma 1, art. 146 del Codice, vale a dire quando attendere i tempi previsti dall'interpello preventivo potrebbe provocare un pregiudizio imminente ed irreparabile.

Sul piano della tipologia delle decisioni va comunque sottolineato un incremento dei casi di accoglimento (totale o parziale) delle richieste dei ricorrenti (15%). In aumento è anche la percentuale delle decisioni dichiarate inammissibili – ivi comprese quelle per mancata regolarizzazione ai sensi dell'art. 148, comma 2, del Codice - (11%), mentre rimane invariata la percentuale delle decisioni dichiarate infondate (14%) (cfr. sez. IV, tab. 4).

Non meno significativo è il dato relativo alle principali caregorie di titolari del trattamento, sia pubblici che privati: in primo luogo gli editori (anche televisivi), le banche e società finanziarie, le società di informazioni commerciali, le Amministrazioni pubbliche e concessionari di servizi pubblici, i fornitori telefonici e telematici, le compagnie di assicurazione, le strutture sanitarie pubbliche e private, gli amministratori condominiali, i liberi professionisti, i datori di lavoro pubblici e privati (cfr. sez. IV, tab. 5).

Tale casistica riflette le difficoltà occupazionali e i profili di criticità del settore lavoristico ed evidenzia la configurazione di un "nuovo" contenzioso (messo in risalto anche nella precedente Relazione) rispetto all'utilizzo delle moderne tecnologie e la ricerca del delicato equilibrio fra tutela della riservatezza dei singoli e le esigenze organizzative del datore di lavoro.

19.3. *La casistica più significativa*

Nel 2015, risulta consolidata la tendenza, già rilevata come tale negli anni precedenti, di un aumento dei ricorsi in materia di lavoro, legati in particolar modo alla fase patologica ovvero alla cessazione del rapporto. Tali fattispecie si sono per lo più contraddistinte per l'utilizzo, da parte del datore di lavoro, di dati personali del dipendente connessi allo svolgimento dell'attività lavorativa, con particolare riguardo a quelli relativi alle comunicazioni avvenute tramite *account* di posta elettronica aziendale contenente il nome e cognome del dipendente stesso.

In tale ambito meritano una particolare attenzione, tra gli altri, alcuni casi che, pur avendo come base comune l'affermato indebito utilizzo, per finalità di controllo, da parte del datore di lavoro dei dispositivi assegnati al dipendente per lo svolgimento della propria attività lavorativa, presentavano elementi specifici ed ulteriori.

Tra questi il ricorso proposto da un avvocato legato da un rapporto di collaborazione ad uno studio legale associato rispetto al quale, pur potendosi ravvisare alcuni

19

tratti tipici del rapporto di lavoro dipendente (quali la suddivisione interna del lavoro per aree di competenza, la gestione centralizzara delle incombenze amministrative, l'utilizzo di strumenti lavorativi dello studio con assegnazione di *account* di posta elettronica facenti capo allo studio stesso, seppur individualizzati mediante l'utilizzo del nome e cognome dell'utente), vi erano comunque elementi di divetsità dati dal fatto che ciascun collaboratore godeva anche di un margine di autonomia nella gestione della propria attività. Il ricorrente ha, in particolare, lamentato l'illegittimo perdurante utilizzo da parte dello studio resisrente, per il tempo successivo al venir meno del rapporto di collaborazione tra le parti, dell'*account* di posta elettronica al medesimo assegnato e contenente i suoi dati identificativi, eccependo peraltro che gli sarebbe stato altresì impedito di accedere ai dati contenuti nel predetto *account*. Lo studio resistente ha precisato che nel proprio disciplinare interno, facente parte del complessivo assetto contrattuale tra quest'ultimo e i propri collaboratori, qualsiasi indirizzo di posta elettronica deve risultare composto dal nome e cognome dell'assegnatario seguito dall'indicazione dello studio e qualificabile come strumento di lavoro di proprietà del datore del lavoro. L'Autorità, facendo applicazione dei princìpi generali contenuti nel provvedimento 1° marzo 2007, Linee guida del Garante per posta elettronica e internet (n. 13, doc. web n. 1387522), ha accolto il ricorso (provv. 5 marzo 2015, n. 136, doc. web n. 3985524) ordinando allo studio legale resistente la disattivazione dell'*account* di posta elettronica contenente i dati identificativi del ricorrente con contestuale utilizzo di un risponditore automatico volto ad avvisare gli utenti dell'avvenuta disattivazione, indicando altresì un indirizzo di posta elettronica aziendale alternativo cui inviare i messaggi attinenti l'attività svolta dallo studio. L'Autorità ha altresì disposto la sospensione immediata di qualunque procedura atta a consentire, in assenza dell'interessato, la consultazione del contenuto dei messaggi, già pervenuti o che sarebbero potuti pervenire sino all'attuazione del provvedimento. Al ricorrente è stato inoltre garantito l'accesso al contenuto dei predetti messaggi al fine di individuare quelli aventi carattere privato o che, pur collegati alla sfera professionale, fossero relativi a rapporti che, in base all'accordo raggiunto tra le parti al termine della collaborazione, continuassero ad essere curati dal medesimo e di poter così verificare l'avvenuta successiva cancellazione dei predetti messaggi da parte del titolare del trattamento.

Altro caso singolare, sempre in ambito lavoristico, è stato quello di una dipendente, licenziata per affermata condotta infedele la quale ha lamentato l'illecita acquisizione da parte del datore di lavoro delle conversazioni avvenute con alcuni clienti e/o fornitori dell'azienda presso cui era impiegata mediante l'utilizzo di Skype, in parte avvenute al di fuori del luogo di lavoro e alla base del predetto licenziamento. Il datore di lavoro, per sua stessa ammissione, aveva provveduto ad installare sul computer assegnato alla dipendente un *software* in grado di visualizzare sia le conversazioni effettuate dalla ricorrente dalla propria postazione, sia quelle avvenute successivamente all'uscita dall'azienda da un computer collocato presso la propria abitazione. Tale condotta è stata riconosciuta dall'Autorità in contrasto con i princìpi posti dalle citate Linee guida del 1° marzo 2007, con le disposizioni più generalmente poste dall'ordinamento a tutela della segretezza delle comunicazioni (v. art. 15 Cost. e artt. 616 ss. c.p.), nonché con la stessa *policy* aziendale adottata a riguardo dal titolare del trattamento e specificamente approvata negli stessi termini dalla competente Direzione territoriale del lavoro. Il ricorso è stato pertanto accolto (provv. 4 giugno 2015, n. 345, doc. web n. 4211000), disponendo per il datore di lavoro il divieto di trattare ulteriormente i dati illecitamente acquisiti, prevedendone la sola conservazione ai fini dell'eventuale acquisizione da parte dell'autorità giudiziaria. Occorre infatti tener presente che il contenuto delle comunicazioni di tipo

elettronico e/o telematico sono assistite da garanzie di segretezza, tutelate anche a livello costituzionale, dirette a consentire, anche in ambito lavorativo, l'esplicazione della persona umana e dunque ad impedire, in attuazione dei princìpi di necessità, correttezza, pertinenza e non eccedenza, un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale. Ciò vale, a maggior ragione, con riferimento a conversazioni che avvengano al di fuori del contesto lavorativo, come verificatosi nel caso di specie.

Da ultimo si riporta il caso significativo di un addetto alla biglietteria presso una compagnia di navigazione, il cui datore di lavoro avrebbe utilizzato i dati registrati dalle telecamere di sorveglianza nell'ambito del procedimento disciplinare e del successivo licenziamento per giusta causa. Il ricorrente ha chiesto il blocco e la cancellazione dei dati per essere stati illecitamente acquisiti, utilizzati e comunque conservati per un periodo superiore a quello consentito dalla legge. Nel corso del procedimento la società resistente ha precisato che l'installazione delle telecamere a circuito chiuso presso le biglietterie è volta ad elevare lo *standard* di sicurezza nelle biglietterie, potenzialmente esposte a rischi connessi alla costante detenzione di denaro contante, nonché ad assicurare agli addetti la possibilità di riscontri oggettivi rispetto a reclami della clientela. Inoltre, la compagnia ha ammesso di aver conservato le immagini registrate per un periodo di novanta giorni, e quindi per un periodo superiore al termine di conservazione previsto dal provvedimento del Garante in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680), senza aver previamente ottenuto un provvedimento, in sede di verifica preliminare ai sensi dell'art. 17 del Codice, di autorizzazione alla conservazione delle immagini per un tempo più lungo di quello consentito dalla legge. L'Autorità ha pertanto accolto il ricorso disponendo, quale misura a tutela dei diritti dell'interessato, il divieto per la società resistente di trattare ulteriormente i dati personali del ricorrente, salva la loro conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria.

Anche nel 2015 numerosi sono stati i ricorsi (50) riguardanti richieste di deindicizzazione dal motore di ricerca Google di notizie riportanti dati non più di interesse pubblico. Com'è noto con la sentenza CGUE (C-131/12, 13 maggio 2013) la Corte ha riconosciuto la società statunitense titolare del trattamento dei dati personali che appaiono nell'elenco dei risultati del suo motore di ricerca, riconoscendo il diritto all'interessato di rivolgersi al gestore del motore di ricerca al fine di ottenere la deindicizzazione dei risultati ottenuti. Di fronte al diniego di Google gli utenti italiani possono rivolgersi in appello al Garante o all'autorità giudiziaria.

Una opportunità, quella del ricorso al Garante, sfruttata finora da un esiguo numero di persone di fronte alle migliaia di istanze rigettate dalla società di Mountain View. In circa un terzo dei casi definiti, il Garante ha accolto le richieste degli interessati ordinando a Google la rimozione dei *link* a pagine presenti sul web che riportavano dati personali ritenuti non più di interesse pubblico, informazioni spesso eccedenti, riferite anche a persone estranee alla vicenda giudiziaria narrata, o lesive della sfera privata. In tutti gli altri casi, invece, l'Autorità ha respinto le richieste ritenendo che la posizione di Google fosse corretta, risultando prevalente l'interesse pubblico ad accedere alle informazioni tramite motori di ricerca. Si trattava, infatti, in prevalenza, di vicende processuali di sicuro interesse pubblico, anche a livello locale, spesso recenti o per le quali non erano ancora stati esperiti tutti i gradi di giudizio. I dati personali riportati, tra l'altro, risultavano trattati nel rispetto del principio di essenzialità dell'informazione.

20 Il contenzioso giurisdizionale

20.1. *Considerazioni generali*

Come riferito in precedenti Relazioni, il d.lgs. n. 150/2011 con l'art. 34 ha abrogato l'art. 152 del Codice – con l'eccezione del comma 1 – dettando all'art. 10 nuove regole procedurali concernenti le controversie in materia di applicazione delle disposizioni del Codice. In particolare, l'art. 34 ha abrogato il comma 7 dell'art. 152, che prevedeva esplicitamente l'obbligo della notifica al Garante dei ricorsi proposti direttamente davanti all'autorità giudiziaria, non coinvolgenti le pronunce dell'Autorità.

Tale abrogazione continua a far sentire i suoi effetti negativi sul numero delle notifiche relative a tale tipologia di giudizi, che in alcuni casi l'autorità giudiziaria ha continuato a ritenere necessarie: a fronte dei 32 ricorsi notificati nel 2013 e dei 31 nel 2014, nel 2015 sono stati notificati, e da questa trattati, 19 ricorsi.

Attesa l'accertata validità di tale strumento a disposizione degli interessati, volto alla tutela giurisdizionale del diritto alla protezione dei dati personali in alternativa al ricorso presentato in sede amministrativa al Garante, assume sempre maggiore rilevanza l'obbligo – purtroppo non sempre puntualmente adempiuto per le cancellerie di trasmettere al Garante copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica (art. 154, comma 6).

Tale obbligo, unitamente alle notifiche dei ricorsi proposti direttamente davanti al giudice che l'autorità giudiziaria riterrà di effettuare, potrà consentire all'Autorità di continuare ad avere conoscenza dell'evoluzione della giurisprudenza in materia di protezione dei dati personali e di segnalare al Parlamento e al Governo degli interventi normativi necessari per la tutela dei diritti degli interessati (come previsto dall'art. 154, comma 1, lett. *f*), del Codice).

20.2. *I profili procedurali*

In tema di giurisdizione, il Tribunale di Bologna, pronunciandosi su una questione relativa al contributo spese per l'esercizio dei diritti previsti dall'art. 7 del Codice di cui nel seguito si dà conto più in dettaglio – ha ribadito che gli artt. 151 e 152 del Codice non lasciano margini a dubbi circa la volontà del legislatore di attribuire l'intera materia alla cognizione dell'A.G.O. senza eccezioni di sorta (26 gennaio 2015, n. 2841).

Vi è stata, inoltre, una pronuncia del Tribunale di Tivoli che si è dichiarato incompetente in favore del Tribunale di Milano, per il trattamento effettuato da una testata giornalistica ivi avente sede, ai sensi dell'art. 10, comma 2, d.lgs. n. 150/2001 come richiamato dall'art. 152 e ss. del Codice, che prevede la competenza esclusiva del tribunale del luogo in cui ha residenza il titolare del trattamento dei dati (13 marzo 2015, n. 620).

In altro caso la Corte di Cassazione ha annullato una sentenza di primo grado del Tribunale di Latina riguardante l'impugnazione di un'ordinanza ingiunzione

emessa dal Garante, rinviando allo stesso Tribunale in persona di diverso magistrato, in quanto il ricorso e il pedissequo decreto di fissazione dell'udienza non erano mai stati notificati al Garante, come invece previsto espressamente dall'art. 152, comma 7 del Codice (13 maggio 2015, n. 9818).

Non si sono riscontrate pronunce che hanno dichiarato un difetto di competenza per materia.

20.3. *Le opposizioni ai provvedimenti del Garante*

L'anno 2015 ha registrato un incremento delle opposizioni a provvedimenti dell'Autorità: a fronte degli 80 ricorsi del 2014, nel 2015 sono state proposte 85 opposizioni. Di queste, 45 si riferiscono a ordinanze ingiunzioni (di cui 2 a verbale di contestazione, inammissibili per costante giurisprudenza e 3 a cartella esattoriale), con una sostanziale stabilità rispetto al 2014, nel quale le impugnazioni di tale natura erano state 44.

Opposizioni a ordinanze ingiunzioni

Complessivamente l'Autorità ha avuto notizia di 42 decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante, che si è sempre costituito tramite l'Avvocatura dello Stato territorialmente competente.

Ventisei sentenze hanno avuto ad oggetto opposizioni ad ordinanze ingiunzioni; in prevalenza, si è trattato di violazioni dell'art. 13 del Codice (omessa o inidonea informativa agli interessati), talvolta unitamente alla mancata acquisizione del consenso e, più raramente, ad altre violazioni della normativa in materia di protezione dei dati personali.

Informativa e consenso

Tra le opposizioni alle ordinanze ingiunzioni, 5 decisioni hanno riguardato sanzioni irrogate in relazione alla raccolta di dati personali da parte di alcune aziende attraverso siti internet, in assenza di un'idonea informativa e, in 2 casi, anche del consenso. Tutte le pronunce, avvalorando la giurisprudenza costante, hanno confermato le valutazioni dell'Autorità e rigettato i ricorsi, nel primo caso con riduzione della sanzione (Trib. Roma, 24 marzo 2015, n. 6679; Trib. Lecce, 9 gennaio 2015 n. 61; Trib. Cagliari, 1° aprile 2015 n. 1074; Trib. Pavia, 13 agosto 2015 n. 278; Trib. Napoli, 19 maggio 2015 n. 7531).

Altre 3 opposizioni hanno avuto ad oggetto il trattamento dei dati in relazione a comunicazioni telefoniche indesiderate a carattere promozionale.

In un primo caso il giudice ha confermato il provvedimento del Garante in relazione all'illecito trattamento compiuto da una società che aveva effettuato chiamate promozionali in assenza di informativa e consenso (Trib. Trani, 23 settembre 2014, n. 1550).

Nel secondo caso, la società ricorrente ha effettuato comunicazioni commerciali estraendo il numero da un elenco telefonico consultabile da chiunque, senza previo consenso. Anche in questo caso, il giudice ha confermato il provvedimento del Garante (Ttib. Roma, 3 ottobre 2014, n.19536).

Nel terzo caso, la società ricorrente ha effettuato telefonate promozionali celando l'identità del chiamante e senza fornire un recapito per esercitare i diritti di cui all'arr. 7 del Codice. Il Tribunale di Torino ha accolto il ricorso in quanto non ha ritenuto adeguatamente provata l'esistenza della fattispecie configurante l'illecito amministrativo ed ha conseguentemente annullato l'ordinanza ingiunzione (24 aprile 2015, n. 2676).

Riscontrando la mancanza di informativa e di consenso, il Tribunale di Roma ha confermato il provvedimento ingiuntivo in relazione al trattamento dati degli operatori di un *call center* di prenotazioni telefoniche di prestazioni sanitarie (21 luglio 2015, n. 16083).

In un'altra pronuncia il Tribunale di Roma ha confermato il provvedimento sanzionatorio del Garante nei confronti di un professionista che, senza il consenso dell'interessata, aveva inviato la richiesta del compenso contenente i dati della propria cliente al datore di lavoro di quest'ultima presso il suo luogo di lavoro (14 maggio 2015, n. 10724).

Due sentenze hanno riguardato l'attivazione di una pluralità di schede telefoniche effettuate da due distinte società nei confronti di singoli interessati senza aver reso loro l'informativa. In entrambi i casi il Tribunale ha confermato il provvedimento del Garante e in un caso ha ridotto la sanzione poiché la violazione è risultata aver avuto ad oggetto tre dei soggetti coinvolti, non sussistendo sufficienti elementi per gli altri due (Trib. Padova, 29 maggio 2015 n. 1590 e Trib. Brescia, 29 ottobre 2015 n. 3076).

In due sentenze i giudici hanno affrontato il tema del termine di 90 giorni – previsto dall'art. 14, l. n. 689/1981 per la contestazione delle violazioni. Entrambi i ricorsi sono stati accolti, uno promosso da una casa di cura alla quale era stata notificata un'ordinanza ingiunzione in relazione alla comunicazione a terzi di dati sensibili in assenza di consenso e l'altro dal legale rappresentate di una società alla quale era stata contestata la pubblicazione *online* di elenchi telefonici in assenza di informativa e consenso. Infatti, anche considerando che, secondo giurisprudenza costante, ai fini dell'individuazione del *dies a quo* deve ritenersi compreso il tempo necessario alla valutazione degli elementi acquisiti all'esito dell'istruttoria, nei casi di specie il termine decadenziale dei 90 giorni è stato ritenuto spirato (Trib. Padova, 1° ottobre 2015, n. 2581 e Trib. Siracusa, 2 marzo 2015, n. 437). Il Garante ha proposto ricorso per Cassazione.

In un caso la Cassazione, su ricorso del Garante che si era visto annullare dal Tribunale di Palmi un'ordinanza ingiunzione per omessa informativa *ex* art. 13 del Codice, emessa nei confronti di un esercizio commerciale che effettuava attività di videosorveglianza, ha affrontato il tema della nozione di dato personale. Il giudice di primo grado aveva ritenuto che l'immagine di una persona, pur possedendo capacità identificativa del soggetto, quando viene trattata integra la nozione di dato personale non automaticamente, ma soltanto qualora chi esegue il trattamento la correli espressamente ad una persona mediante didascalia o altra modalità da cui sia possibile identificarla. La Corte, con significativa innovazione rispetto a precedente decisione, ha condiviso l'argomentazione del Garante, circa il fatto che l'immagine costituisca dato personale, rilevante ai sensi dell'art. 4, comma 1, lett. *b*), del Codice, a prescindere dalla sua notorietà, disponendo, pertanto, la cassazione della sentenza impugnata e il rigetto dell'opposizione proposta dal ricorrente in primo grado (2 settembre 2015, n. 17440).

Notificazione

La Cassazione, adita da un laboratorio di analisi cliniche che si era visto confermare dal Tribunale di Foggia un'ordinanza ingiunzione per omessa norificazione emessa nei suoi confronti, ha dichiarato inammissibile il ricorso, in quanto, come rilevato in sede di controricorso dall'Autorità, nessuno dei motivi che prospettava vizi di violazione e falsa applicazione di legge poneva, come richiesto dalla (previgente) formulazione dall'art. 366-*bis* c.p.c. "*...un quesito che individui tanto il principio di diritto che è alla base del provvedimento impugnato, quanto, correlativamente, il principio di diritto, diverso dal precedente, la cui auspicata applicazione ad opera della Corte medesima possa condurre ad una decisione di segno inverso rispetto a quella impugnata*" (12 marzo 2015, n. 4977).

Con riferimento ad un'opposizione proposta da una casa di cura avverso un'ordinanza ingiunzione adottata a seguito della violazione dell'obbligo di notificazione del trattamento di dati sensibili il Tribunale di Firenze ha confermato il provvedi-

mento del Garante, ritenendo che allo spostamento della sede legale della società interessata non era seguita alcuna notifica al Garante e che la stessa società, di nuovo senza notificare, aveva cessato l'attività di cura e di ricovero e sala operatoria (8 gennaio 2015, n. 29).

In un'altra pronuncia una società è stata sanzionata per aver omesso di notificare al Garante l'effettuazione di trattamenti di dati genetici e di dati idonei a rilevare lo stato di salute e la vita sessuale. L'organo giudicante ha confermato il provvedimento impugnato, non ritenendo sufficienti le motivazioni della suddetta società riguardo alla buona fede e la mancanza di colpa, trattandosi di un laboratorio di analisi e non di "esercenti le professioni sanitarie" sottratti all'obbligo di notifica sussistendo determinate condizioni (Trib. Brindisi, 18 dicembre 2014, n. 2165).

Tre opposizioni hanno riguardato il trattamento dati da parte di soggetti pubblici.

Trattamento dati da parte di soggetti pubblici

In due casi si è trattato di pubblicazione di dati sulla salute da parte rispettivamente di un Comune sul proprio sito web e di un'Azienda ospedaliera sulla bacheca di un reparto e per entrambi l'organo giudicante ha accolto il ricorso e revocato il provvedimento del Garante. In un caso il Tribunale ha ritenuto il Comune incolpevole a fronte di un contesto normativo incerto al momento della condotta lesiva, mancando un raccordo tra le disposizioni concernenti la tutela della *privacy* e quelle relative agli obblighi di trasparenza (Trib. Aosta, 17 novembre 2015 n. 394). Nell'altro caso il giudice si è soffermato sulla nozione di dato sensibile, ritenendo che nel caso di specie le espressioni contenute in una nota esposta in bacheca non fossero qualificabili come dato sensibile in quanto non idonee a rivelare lo stato di salute dell'interessato (Trib. Cuneo, 27 giugno 2015, n.152). Per la seconda sentenza il Garante ha proposto ricorso in Cassazione.

La Cassazione ha poi accolto in parte il ricorso presentato da un Comune che aveva notificato un'ordinanza ingiunzione di pagamento presso il domicilio del destinatario ma non in busta chiusa e nelle mani di un terzo estraneo. La sentenza di primo grado, confermando il provvedimento del Garante, aveva accertato la violazione contestata riconoscendo all'interessato un risarcimento del danno che la Cassazione ha ritenuto non sufficientemente dimostrato, essendo il danno stesso stato identificato dal Tribunale nell'illecito trattamento e non individuato come conseguenza di esso (5 settembre 2014, n. 18812).

Cartella esattoriale

Il Tribunale di Milano ha respinto il ricorso proposto da una società avverso la cartella esattoriale emessa dall'agente riscossore nell'interesse del Garante a seguito del mancato pagamento della somma ingiunta, riconoscendo che l'ordinanza ingiunzione costituisce titolo esecutivo e dunque il Garante aveva correttamente applicato le maggiorazioni che, diversamente da quanto sostenuto da parte attrice, non decorrevano dal momento in cui era passata in giudicato la sentenza che aveva confermato il suddetto provvedimento ingiuntivo (16 gennaio 2015, n. 2006).

Lavoro

Con riguardo al trattamento dei dati sul luogo di lavoro, una decisione del Tribunale di Latina ha riguardato la diffusione della notizia della rimozione di una dipendente di un ente pubblico dalle funzioni cui era preposta nonché la consegna a mano – da persona non incaricata del trattamento – del provvedimento non inserito in busta o plico. Il Garante, nel caso di specie, non aveva riscontrato violazioni, avendo ritenuto che la consegna delle note dirigenziali fosse stata eseguita da un'incaricata che poteva legittimamente prenderne conoscenza anche in base ad un ordine di servizio, mentre la diffusione ad altri soggetti della notizia non è emersa dagli accertamenti effettuati (provv. 18 ottobre 2012, n. 296, doc. web n. 2174351). Il Tribunale, dopo aver esaminato la questione della competenza territoriale, ha affermato che le informazioni relative alla revoca da una determinata posizione organizzativa costituiscono dati personali. In particolare la menzionata con-

dotta è stata ritenuta violativa del Codice sia per quanto attiene alla regola cautelare che impone misure minime onde evitare l'indebita diffusione delle informazioni personali, sia con riferimento alla prescrizione prevista dalle Linee guida in materia di impiego pubblico del 14 giugno 2007 (doc. web n. 1417809), secondo cui l'amministrazione deve utilizzare forme di comunicazione individualizzate con il lavoratore, adottando le misure più opportune per prevenire la conoscibilità da parte di soggetti diversi dal destinatario (9 settembre 2015, n. 1792).

Avverso tale decisione è pendente ricorso in Cassazione proposto dal Garante.

In altro caso, il Tribunale di Catanzaro ha confermato le argomentazioni del Garante contenute nel provvedimento 4 ottobre 2013, n. 469 (doc. web n. 2799174) circa il trattamento illecito posto in essere da un ente locale in riferimento alla consultazione da parte di alcuni dirigenti del fascicolo personale, conrenente anche dati sensibili, di una dipendente. Il Garante aveva in particolare ritenuto che i dati oggetto di comunicazione, effettuata a soggetti non incaricati del trattamento, non fossero pertinenti rispetto alle finalità per le quali erano stati raccolti e poi trattati, né indispensabili per lo svolgimento delle attività istituzionali (1° giugno 2015, n. 857).

Giornalismo

La Corte di Cassazione si è pronunciara circa la legittimità del provvedimento del Garante 15 luglio 2006 (doc. web n. 1310796) che aveva vietato, in via preventiva, la diffusione di dati personali di carattere sanitario di un personaggio pubblico, vittima di un incidente stradale e sul quale il Tribunale di Milano, condividendo la tesi del Garante, aveva ritenuto in prima istanza violato il principio di essenzialità dell'informazione. La Cassazione, in particolare con riferimento ad una questione sulla conformità all'art. 21 della Costituzione dei poteri attribuiti al Garante, ha ribadito che la tutela preventiva e inibitoria posta in essere nel caso di specie è del tutto legittima ai sensi dell'art. 143, lett. *c)* del Codice nell'ipotesi in cui "vi sia il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati" (16 aprile 2015, n. 7755).

In altro caso, il giudice confermando il provvedimento del Garante dell'11 settembre 2014, n. 400 (doc. web n. 3405138) riguardante la diffusione di notizie raccolte da un giornalista, rramite un imitatore che, telefonando ad un personaggio pubblico, si era fatto passare per persona amica e di fiducia dell'interlocutore ha sostenuto che il giornalista non può utilizzare artifici e raggiri per raccogliere notizie che potrebbero essere acquisite con gli strumenti propri dell'inchiesta giornalistica.

In tal senso, il Garante aveva ritenuto l'acquisizione e la successiva messa in onda della conversazione telefonica non conforme ai princìpi e alle norme del codice deontologico dei giornalisti e del Codice, vietandone l'ulteriore diffusione Il Tribunale di Milano ha in particolare evidenziato che l'esimente prevista dal codice deontologico relativa alla possibilità di omettere l'informativa richiede che sia provata l'impossibilità di esercizio in altro modo della funzione informativa e che non erano stati allegari specifici elementi dai quali desumere quanto affermato (4 giugno 2015, n. 6968).

Accesso ai dati personali

Il Tribunale di Pisa ha confermato il provvedimento del Garante 17 aprile 2014, n. 213, (doc. web n. 3259462*)* con il quale era srato ordinato ad un istituto bancario di comunicare i dati riguardanti un cliente che aveva ricevuto un riscontro inidoneo alla propria richiesta di accesso ai dati personali, distinguendo tale diritto da quello di accesso alla documentazione bancaria previsto dal t.u. bancario (28 ottobre 2015, n. 1212).

In un'altra pronuncia, il Tribunale di Pesaro ha negato che la società ricorrente potesse invocare la tutela di cui all'art. 7 del Codice, in quanto con modifica legislativa del 2011 sono state espressamente sottratte alla predetta disciplina le persone giuridiche; ciò benché secondo una sentenza della CGUE (nelle cause riunite C-

92/09 e C-93/09, Volker und Markus Schecke GbR e Hartmut Eifert / Land Hessen) le persone giuridiche possano invocare la tutela degli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE allorché la loro ragione sociale identifichi una o più persone fisiche, come nel caso della ricorrente società; tale sentenza, ha evidenziato il Tribunale, non ha espresso un principio di carattere generale, trattandosi invece di materia del tutto diversa da quello in esame (29 ottobre 2015 n. 812).

Vi sono state infine decisioni relative a materie diverse ed eterogenee.

Altre pronunce

Il Tribunale di Santa Maria Capua Vetere ha accolto il ricorso di un amministratore di condominio destinatario di un'ordinanza ingiunzione in relazione alla mancata risposta ad una richiesta di informazioni da parte del Garante circa l'affissione nella bacheca condominiale di un provvedimento comunale di sgombro contenente dati personali. Il Tribunale, ritenendo che gli obblighi collaborativi del privato nel procedimento innanzi al Garante sono finalizzati a comprimere il tempo e l'intensità della presunta violazione, ha deciso che la mancata spontanea collaborazione del ricorrente non avesse comportaro un aggravio nella definizione della procedura, se non per la tempistica, in quanto, a seguito dell'ispezione effettuata *in loco,* era stata verificata la cessazione della condotta contestata e non erano stati ravvisati gli estremi per adottare un provvedimento del Garante (30 aprile 2015, n. 1607). Avverso tale sentenza è stato proposto dal Garante ricorso per Cassazione.

Il Tribunale di Catania ha accolto il ricorso proposto da una società destinataria di un provvedimento ingiuntivo per avere trattato dati biometrici al fine di rilevare le presenze dei propri dipendenti in assenza di informativa e consenso e senza aver provveduto alla prevista notificazione al Garanre. La società aveva motivato tale condotta sostenendo che, nel caso specifico, non vi era alcun trattamento di dati biometrici, essendo i suddetti dati utilizzati solo per accertare che la mano che usa il *badge* sia la stessa utilizzata per configurare il *badge*, poiché l'apparecchiatura tecnica utilizzata non permette l'identificazione della persona (15 maggio 2015, n. 2164). Avverso tale sentenza è pendete ricorso in Cassazione proposto dal Garante.

Un'altta decisione ha accolto il ricorso della responsabile del trattamento dati di un centro per l'impiego in relazione alla mancata adozione delle misure di sicurezza, in riferimento alla giacenza, presso un cassone, di materiale contenente dati sensibili, destinato allo scarto d'archivio. Il Tribunale ha precisato che la norma del Codice punisce espressamente il titolare del trattamento, sicché non è ammissibile un'interpretazione estensiva riferita al responsabile, al quale invece può imputatsi la violazione solo se abbia disatteso le indicazioni ricevute dal titolare, evento che nel caso concreto non si è verificato. Inoltre, dalla contestata violazione era scaturito anche un procedimenro penale conclusosi con sentenza di assolvimento, ulteriore conferma della insussistenza della medesima violazione sul piano della sanzione amministrativa (Trib. Savona, 12 dicembre 2014, n. 1645).

Il Tribunale di Napoli ha confermato il provvedimento del Garante che ha prescritto, tra l'altro, ad una società di adottare soluzioni informatiche idonee ad assicurare il controllo delle attività svolte dagli incaricati del trattramento sui dati di traffico telefonico, anche mediante registrazione delle operazioni compiute in un apposito *audit log* (provv. del 17 gennaio 2008, doc. web n. 3136961). Il Tribunale ha respinto il ricorso della socierà, riconoscendo che il potere di imporre prescrizioni in materia di traffico telefonico si fonda sul provvedimento che, al par. 7.6, prevede esplicitamente la misura prescritta dal provvedimento impugnato (5 novembre 2015, n. 13976).

Anche in un altro caso, inerente l'invio, da parte di una società, di comunicazioni indesiderate di carattere promozionale via fax in assenza di consenso, è stato integralmente confermato il provvedimento del Garante 23 gennaio 2014, n. 30

(doc. web n. 2927848) (Trib. Milano, 23 aprile 2015, n. 5192).

Il Tribunale di Ivrea ha confermato un provvedimento del Garante 2 dicembre 2010 (doc. web n. 1784000) che ha dichiarato infondato il ricorso amministrativo con il quale l'interessato lamentava l'illiceità acquisizione, da parte di una società telefonica, dei dati relativi a depositi bancari a lui intestati, utilizzati allo scopo di promuovere una procedura di pignoramento per il recupero delle ingenti somme dovute dal ricorrente per fatture non pagate. In particolare, il giudice ha confermato l'assunto del Garante, secondo cui da un lato la normativa di tutela dei dati personali consente il trattamento effettuato per far valere o difendere un diritto in sede giudiziaria e per detto trattamento non è richiesta né l'informativa all'interessato (art. 13 comma 5, lett. *b*) né il suo consenso (art. 24 comma 1, lett. *f*); e, dall'altro, a mente dell'art. 160 del Codice, la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale, con ciò escludendo, *tout court,* la competenza del Garante a valutare l'eventuale illiceità del trattamento dei dati presentati all' A.G.O. (29 novembre 2011, n. 639).

Il Tribunale di Roma, in una sentenza di rigetto avverso un provvedimento dell'Autorità in materia di ttattamento di dati personali sullo stato di salute del 23 dicembre 2010 (doc. web n. 1800931), ha ptecisato che, con esclusione della diffusione, la tutela della riservatezza deve necessariamente affievolire in presenza di dati già divulgati dallo stesso interessato, che, di fatto, concretizza una forma di consenso implicito al loro trattamento (15 ottobre 2014, n. 19822). Avverso tale sentenza è stato proposto ricorso per Cassazione.

Lo stesso Tribunale, in altra pronuncia, ha confermato un altro provvedimento del Garante 19 giugno 2014 che aveva dichiarato infondato il ricorso contro un'asseritamente erronea segnalazione alla Centrale rischi, rilevando che il procedimento avviato ai sensi dell'art. 152 del Codice, è volto alla verifica della legittimità del trattamento dei dati personali e non può essere utilizzato per l'accertamento dei rapporti di credito intercorrenti tra i ricorrenti (18 giugno 2015, n. 13414).

Anche in altro caso, inerente il trattamento di dati giudiziari da parte di un soggetto pubblico, e, in particolare, la pubblicazione sul sito internet del decreto di rinvio a giudizio nei confronti, tra l'altro, di un candidato alle elezioni dell'organo collegiale dell'ente pubblico ricorrente, è stato integralmente confermato il provvedimento del Garante 17 gennaio 2013, n. 15 (doc. web n. 2315622). Il giudice, condividendo la tesi dell'Autorità, ha ritenuto che nel caso di specie non si era trattato di un trattamento per finalità elettorali espressamente previste tra quelle di interesse pubblico dal codice e dal tegolamento adottato dall'ente pubblico interessato, bensì di vera e propria propaganda elettorale attraverso una diffusione indiscriminata dei suddetti dati (Trib. Roma, 28 aprile 2015, n. 9346).

Il Tribunale di Napoli ha respinto il ricorso proposto da un esercizio commerciale contro il provvedimento del Garante 4 luglio 2013, n. 335 (doc. web n. 2577227) che aveva dichiarato illecito il trattamento dati effettuato con un sistema di videosorveglianza installato presso detto locale, accompagnato da un'informativa inidonea e posta in luogo non visibile all'esterno, in assenza di nomina del responsabile e/o incaricato del trattamento e di istruzioni circa le operazioni di trattamento effettuate. L'organo giudicante, preso atto del sopravvenuto adempimento da parte del ricorrente e del provvedimento di parziale annullamento del Garante, ha confermato per la parte restante il provvedimento, sostenendo che l'adempimento delle prescrizioni non elideva il carattere illecito del trattamento rendendo solo lecito, da quel momento in poi, ciò che in precedenza non lo era (20 gennaio 2015, n. 1534).

Infine il Tribunale di Bologna ha annullato il provvedimento del Garante 18 marzo 2010, n. 18 (doc. web n. 1709118) con il quale venivano determinati i casi in cui una società specializzata in sistemi di informazione creditizia poteva chiedere all'interessato un contributo spese per l'esercizio dei diritti di cui all'art. 7 del Codice, fissando altresì un limite massimo a tale contributo. In particolare, il provvedimento contestato prevedeva per talune ipotesi la gratuità del riscontro, per altre la possibilità di chiedere un contributo a carico dell'interessato. Il giudice ha ritenuto che la previsione della gratuità sia contraddittoria in quanto, nel caso in cui "si determina un notevole impiego di mezzi in relazione all'entità [.....] delle richieste", ai sensi dell'art. 10, comma 8 del Codice, è necessario individuare un contributo a favore della società ricorrente. È stato poi rilevato un profilo di irragionevolezza nell'ipotesi di gratuità qualora l'interessato chieda il riscontro via posta elettronica, in quanto "il notevole impiego di mezzi" relativo alla complessità ed entità delle richieste non riguarda tanto le modalità di trasmissione quanto quelle di archiviazione, conservazione, selezione ed estrazione dati (26 gennaio 2015, n. 2841).

20.4. *L'intervento del Garante nei giudizi relativi all'applicazione del Codice*

Conformemente agli indirizzi giurisprudenziali ed al parere espresso dall'Avvocatura generale dello Stato – il Garante, nei giudizi diversi da quelli direttamente attinenti a pronunce dell'Autorità, ha limitato la sua attiva presenza, ai soli casi in cui sorge, o può sorgere, la necessità di difendere o comunque far valere particolari questioni di diritto.

In questo quadro, l'Autorità, nel periodo di riferimento non è intervenuta in giudizio ma ha seguito con attenzione tutti i contenziosi relativi all'applicazione del Codice, chiedendo alle Avvocature distrettuali dello Stato di essere comunque informata sullo svolgimento delle vicende processuali e di ricevere comunicazione in merito agli esiti.

21 L'attività ispettiva e le sanzioni

21.1. *La programmazione dell'attività ispettiva*

L'attività ispettiva è lo strumento istruttorio necessario per accertare *in loco* situazioni di fatto che devono essere oggetto di valutazione da parte dell'Autorità in relazione a specifici casi. Essa però è spesso utilizzata anche con lo scopo di acquisire conoscenze in relazione a fenomeni nuovi in vista di una successiva regolazione da parte del Garante attraverso i cd. provvedimenti generali.

Le ispezioni (303 nel 2015) sono effettuate sulla base di programmi elaborati secondo linee di indirizzo stabilite dal Collegio con delibere di programmazione che indicano gli ambiti del controllo e gli obiettivi numerici da conseguire. Le linee generali della programmazione dell'attività ispetriva vengono quindi rese pubbliche attraverso il sito web del Garante e, sulla base dei criteri così fissati, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo e istruisce i conseguenti procedimenti. Il programma relativo al 2015 ha previsto che l'attività ispettiva fosse, tra l'altro, indirizzata nei seguenti settori:

- ospedali e aziende sanitarie con riferimento alle modalità di attuazione del Fascicolo sanitario elertronico e del *dossier* sanitario;
- società che effettuano artività di *marketing* telefonico mediante *call center* operanti all'estero;
- società che gestiscono sistemi di pagamento su dispositivi portatili (*mobile payment proximity*) ovvero che abilirano pagamenti o trasferimenti di denaro tramite telefono cellulare. L'elemento discriminante del *mobile payment* è l'uso del telefono cellulare come leva di innovazione nel processo di pagamento, indipendentemente dagli strumenti di pagamento utilizzati e dalle tecnologie di comunicazione adottate. Nello specifico il *mobile proximity payment* comprende i pagamenti elerttonici "di prossimità", ovvero pagamenti per cui sia necessaria una vicinanza fisica tra l'acquirente ed il venditore del prodotto/servizio acquistato. Nel *mobile proximity payment* il cellulare emula un pagamento ttamite carta;
- banche, con riferimento alla verifica sull'attuazione delle misure previste nel provvedimento generale relativo alla "tracciabilità delle operazioni bancarie";
- operatori telefonici, con riferimento ai trattamenti effettuati per la gestione dei servizi sms;
- società che forniscono servizi finalizzati alla fidelizzazione della clientela (carte fedeltà, *pay back*);
- attività di *marketing* telefonico effettuato da società, anche con riferimento al rispetto del provvedimento generale sulle cd. chiamate mute;
- centri di assistenza fiscale (caf), per la verifica del rispetto delle misure organizzative e di sicurezza adottate nell'ambito della trasmissione della dichiarazione dei redditi precompilata;
- società che forniscono *software* e servizi tecnologici nell'ambito delle attività di supporto alle indagini.

Come specificato al successivo paragrafo 21.3, nel periodo di riferimento sono state anche effettuate, in altri settori, verifiche:

- sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;
- sull'adempimento dell'obbligo di notificazione da parte di soggetti, pubblici e privati, individuati mediante raffronto con il registro generale dei trattamenti;
- sulla liceità e correttezza dei trattamenti di dati personali, con particolare riferimento al rispetto dell'obbligo di informativa, alla pertinenza e non eccedenza nel trattamento, alla libertà e validità del consenso, nei casi in cui questo è necessario, nonché alla durata della conservazione dei dati nei confronti di soggetti, pubblici o privati, appartenenti a categorie omogenee.

In tutta l'attività è stata prestata specifica attenzione ai profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate.

21.2. *La collaborazione con la Guardia di finanza*

Anche nell'anno di riferimento l'Autorità si è avvalsa della preziosa collaborazione della Guardia di finanza per lo svolgimento dell'attività di controllo in applicazione del protocollo di intesa siglato nel 2005. Al riguardo si fa rinvio a quanto nel dettaglio riferito nelle precedenti edizioni (cfr., da ultimo, Relazione 2009, p. 240 ss.), evidenziando ancora una volta la meritoria attività svolta dal Nucleo speciale *privacy*, che ha provveduto direttamente a effettuare gli accertamenti delegati, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti. Sulla base della prassi operativa ormai consolidata, le informazioni e i documenti acquisiti nell'ambito degli accertamenti dal Corpo sono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei principi previsti dalla legge. Nei casi in cui sono emerse violazioni penali o amministrative, la Guardia di finanza ha provveduto a informare l'autorità giudiziaria competente e ad avviare i procedimenti sanzionatori amministrativi mediante la redazione della "contestazione", in conformità alla l. 24 novembre 1981, n. 689.

Grazie alla sinergia ormai collaudata con il Nucleo speciale *privacy* della Guardia di finanza, il Garante dispone di un dispositivo di controllo flessibile ed articolato, in grado di integrare l'attività ispettiva svolta direttamente dal competente Dipartimento dell'Autorità, consentendo così l'effettuazione, efficace e tempestiva, di tutte le verifiche *in loco* che si rendono necessarie per garantire il rispetto della protezione dei dati personali su tutto il territorio nazionale.

È proseguita l'attività di formazione del personale del Corpo al fine di approfondire la conoscenza delle disposizioni del Codice e dei provvedimenti dell'Autorità: nello specifico sono stati organizzati due seminari presso il Nucleo speciale *privacy* nell'ambito dei quali sono stati esaminati vari profili relativi ai procedimenti sanzionatori, nonché le indicazioni del Garante contenute nel parere sull'accesso alla dichiarazione precompilata da parte del contribuente e degli altri soggetti autorizzati del 19 febbraio 2015, n. 95 (doc. web n. 3741076).

Considerati gli ottimi risultati raggiunti nel rapporto di collaborazione, ormai ultra decennale, tra il Garante e la Guardia di finanza e al fine di tenere conto delle nuove sfide tecnologiche nonché del rilievo sempre maggiore che l'ambito internazionale avrà nelle istruttorie – anche a seguito della definizione del nuovo quadro normativo europeo –, è stato delineato, d'intesa con la Guardia di finanza, il contenuto di un nuovo protocollo d'intesa.

Il nuovo protocollo prevedrà, dal punto di vista strategico, che il Garante possa avvalersi di personale specializzato della Guardia di finanza per la conduzione di

ispezioni congiunte con altre autorità estere (l'introduzione del nuovo regolamento europeo in materia di dati personali, infatti, renderà tale necessità sempre più frequente).

Da un punto di vista più strettamente operativo, invece, il nuovo protocollo garantirà: una sempre maggiore semplificazione dei flussi documentali tra l'Ufficio e il Nucleo speciale *privacy* (attraverso l'uso sistematico di strumenti di trasmissione telematici); l'introduzione di modalità di verifica *online* di possibili violazioni alla normativa in materia di protezione dei dati personali (attraverso l'esame diretto di siti web, senza necessità di ispezioni *in loco*); un coinvolgimento stabile del Nucleo frodi telematiche della Guardia di finanza in attività ispettive o di analisi ad alto contenuto tecnico/informatico.

21.3. *I principali settori oggetto di controllo*

Oltre a quanto già riportato al paragrafo 21.1, nel 2015 le ispezioni effettuate dall'Autorità hanno riguardato i titolari del trattamento che:

- hanno notificato trattamenti di dati personali relativi alla rilevazione della posizione geografica di persone o oggetti mediante una rete di comunicazione elettronica (art. 37, comma 1, lett. *b*) unitamente al trasferimento di dati all'estero, al fine di verificare le tipologie di trattamento effettuate, le misure di sicurezza predisposte, nonché i presupposti giuridici, l'ambito e le modalità del trasferimento di dati personali in Paesi non appartenenti all'Unione europea;
- operano nel settore dei trasporti (ivi incluso il settore del setvizio di trasporto pubblico locale), trattando dati relativi alla geolocalizzazione di veicoli, con particolare riferimento all'utilizzo di tali sistemi nell'ambito del rapporto di lavoro. In questa attività è stata posta particolare attenzione al rispetto delle norme previste dalla disciplina lavoristica (artt. 114 del Codice e 4 della l. n. 300/1970), nonché alla corretta attuazione delle misure e degli accorgimenti prescritti dal Garante nell'ambito del provvedimento generale 4 ottobre 2011, n. 370 (doc. web n. 1850581). Tra questi ricordiamo: la non continuatività – di regola – del monitoraggio della posizione dei veicoli; la commisurazione dei tempi di conservazione delle diverse tipologie di dati trattati alle finalità in concreto perseguite; la designazione quali responsabili del trattamento ai sensi dell'art. 29 del Codice degli operatori economici che forniscono i servizi di localizzazione del veicolo e di trasmissione della posizione del medesimo;
- svolgono attività di *marketing* telefonico tramite *call center* operanri in Paesi al di fuori dell'Unione europea. In particolare, le verifiche in questo settore sono state indirizzate all'acquisizione di informazioni su: strutture societarie dei soggetti interessati; contratti con le società committenti; procedure adottate dal titolare del trattamento per il controllo della filiera e la corretta esecuzione delle istruzioni impartite ai responsabili; misure di sicurezza adottate; artuazione delle misure e degli accorgimenti prescritti dal Garante nell'ambito del provvedimento generale 10 ottobre 2013, n. 444 (doc. web n. 2724806) (tra cui: informativa all'interessato sull'ubicazione dell'operatore, possibilità di scelta di usufruire del servizio attraverso un operatore ubicato sul territorio nazionale, comunicazione al Garante in caso di trasferimento di dati personali ad un *call center* sito al di fuori dell'Unione europea);

- svolgono attività di *marketing* telefonico attraverso l'uso di sistemi automatizzati, con modalità tali da generare il fenomeno delle cd. chiamate mute. In particolare, le verifiche sono state indirizzate all'acquisizione di informazioni su: origine dei dati personali; *call center* utilizzati; società committenti; procedure adottate dal titolare del trattamento per garantire agli interessati l'effettivo esercizio dei diritti di cui all'art. 7 del Codice; adempimento degli obblighi di informativa e raccolta del consenso; attuazione delle misure e degli accorgimenti prescritti dal Garante nell'ambito del provvedimento generale 20 febbraio 2014, n. 83 (doc. web n. 3017499) (in particolare, l'adozione di strumenti di reportistica in grado di rilevare gli indicatori di prestazioni al fine di rispettare la percentuale massima di cd. chiamate mute ed i tempi minimi per la richiamata; i tempi di conservazione dei relativi report; l'adozione del cd. *comfort noise*);
- forniscono servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione, al fine di verificare il rispetto di quanto stabilito dall'art. 132 del Codice, con riferimento alla conservazione dei dati di traffico telefonico e telematico per finalità di prevenzione e accertamento dei reati (cd. *data retention*). In questa attività è stata posta particolare attenzione a: verifica dei dati conservati; rispetto dei termini tassativi di conservazione stabiliti dalla legge (il cui mancato rispetto, oltre a rendere illecito il trattamento, è sanzionato amministrativamente sia in caso di superamento del termine che di conservazione per tempi inferiori a quelli stabiliti dall'art. 132 del Codice); corretta attuazione delle misure e degli accorgimenti prescritti dal Garante nell'ambito del provvedimento 17 gennaio 2008 (doc. web n. 1482111). Tra questi ricordiamo: la limitazione dell'accesso ai dati e ai locali dove gli stessi sono custoditi; il tracciamento dell'attività del personale incaricato di accedere ai dati; la conservazione separata dei dati e la loro cancellazione una volta decorso il termine di conservazione stabilito dalla legge; l'effettuazione di controlli interni sulla legittimità degli accessi ai dati da parte degli incaricati e l'adozione di sistemi di cifratura;
- hanno notificato trattamenti di dati personali relativi al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti (art. 37, comma 1, lett. *f*), unitamente al trasferimento di dati all'estero. In tale ambito i controlli hanno riguardato, tra l'altro: misure di sicurezza adottate, modalità di adempimento dell'obbligo di informativa agli interessati e dell'eventuale raccolta del consenso, presupposti giuridici, ambito e modalità dell'eventuale comunicazione di dati personali a soggetti terzi o del trasferimento degli stessi in Paesi non appartenenti all'Unione europea;
- operano nel settore del commercio di integratori alimentari (anche) mediante l'utilizzo di siti web, al fine di verificare: le tipologie di trattamento effettuate e le relative finalità, le modalità di adempimento dell'obbligo di informativa agli interessati e dell'eventuale raccolta del consenso, nonché i presupposti giuridici, l'ambito e le modalità dell'eventuale comunicazione di dati personali a soggetti terzi;
- operano nel settore della ricezione alberghiera con strutture di categoria elevata o di lusso, al fine di verificare la liceità del trattamento dei dati della clientela, anche con riferimento ai dati raccolti attraverso siti web o attraverso l'utilizzo di sistemi di videosorveglianza, con particolare evidenza per le modalità di rilascio dell'informativa e di raccolta del consenso degli interessati, ove necessario;

- operano nel settore della cura della persona, centri benessere e spa, al fine di verificare la liceità del trattamento dei dati della clientela, anche con riferimento ai dati raccolti attraverso siti web o attraverso l'utilizzo di sistemi di videosorveglianza, con particolare evidenza per le modalità di rilascio dell'informativa e di raccolta del consenso degli interessati, ove necessario;
- offrono servizi finalizzati alla conservazione di cellule cordonali/staminali, unitamente ad altre società che operano al di fuori del territorio italiano. Le verifiche effettuate sono state indirizzate a rilevare le modalità e le finalità del trattamento dei dati personali degli interessati, le misure di sicurezza adottate, le modalità con cui viene resa l'informativa e raccolto il consenso degli interessati, l'adempimento degli obblighi di notificazione (con particolare riferimento ai trattamenti previsti dall'art. 37, lett. *a*) e *b*) del Codice). I controlli sono stati tesi ad appurare, altresì, l'ambito, i presupposti e le modalità dell'eventuale comunicazione di dati personali a società controllanti, collegate o soggetti terzi, nonché il trasferimento degli stessi in Paesi non appartenenti all'Unione europea;
- operano nel settore delle attività sportive (palestre e centri *fitness*) al fine di appurare il rispetto della disciplina in materia di protezione dei dati personali, con particolare riferimento ai profili dell'informativa resa agli interessati (anche in merito al trattamento di dati personali tramite impianti di videosorveglianza o siti web), nonché del consenso acquisito dagli stessi, ove necessario.

Sono stati effettuati altresì controlli nei confronti di specifici titolari del trattamento per esigenze istruttorie connesse alle segnalazioni, ai reclami e ai ricorsi pervenuti all'Autorità.

In relazione a quanto emerso dagli accertamenti, sono stare effettuate numerose proposte di adozione di provvedimenti inibitori e/o prescrizioni per conformare il trattamento alla legge, a fronte delle quali l'Autorità, come riportato nel prossimo paragrafo, ha adottato alcuni provvedimenti particolarmente significarivi per i cittadini.

21.4. *I provvedimenti adottati dall'Autorità a seguito dell'attività ispettiva*

Attraverso le ispezioni l'Autorità svolge una penetrante attività istrutroria che può essere finalizzata, a seconda del caso, a uno o piìn dei seguenti obiettivi:

- intervenire sui trattamenti illeciti da chiunque effettuati adottando i provvedimenti cautelari previsti dalla legge (blocco e diviero) e/o definendo le misure necessarie da prescrivere per rendere il trattametito conforme alla legge (contrasto dell'illecito);
- verificare lo stato di artuazione delle prescrizioni adottate dal Garante nei diversi contesti e sanzionare gli eventuali inadempimenti al fine di prevenire futuri illeciti (attività preventiva);
- acquisire tutti gli elementi utili a comprendere nuovi fenomeni emergenti che impattano notevolmente sul diritto alla protezione dei dati personali degli interessati (ad es., il tema del *mobile remote payment*) in modo da definire tempestivamente le misure e gli accorgimenti che devono essere adottati da tutti i soggetti che sono coinvolti nei trattamenti (attività conoscitiva).

Occorre tenere presente che, al di là della/e finalità che la sottendono, l'ispezione è pur sempre un procedimento amministrativo di controllo all'esito del quale, ove vengano accertate illiceità, l'Autorità è tenuta ad adottare i necessari provvedimenti

per rendere il trattamento conforme alla legge e a contestare le sanzioni eventualmente rilevate.

Con riferimento al 2015, tra i provvedimenti più rilevanti adottati sulla base degli elementi istruttori acquisiti in sede ispettiva si segnalano, in ordine cronologico, quelli con i quali il Garante ha:

- dichiarato illecito e vietato il trattamento dei dati personali effettuato da una società monitorando il traffico in rete di un dipendente, poi licenziato, in violazione delle indicazioni fornite nelle Linee guida per posta elettronica e internet (provv. 1° marzo 2007, n. 13, doc. web n. 1387522), nonché dell'art. 4, l. n. 300/1970, con la conseguente inutilizzabilità dei dati trattati in violazione di legge, ai sensi dell'art. 11, comma 2 del Codice (provv. 5 febbraio 2015, n. 65, doc. web n. 3813428);
- dichiarato illecito e vietato il trattamento dei dati personali, utilizzati da una società di formazione per attività promozionale effettuata per mezzo dell'invio di posta cartacea, acquisiti senza aver preventivamente informato gli interessati né acquisito il loro consenso per il trattamento (provv. 5 marzo 2015, n. 120, doc. web n. 3871397);
- prescritto a due società di rafforzare le misure di sicurezza, adottate a tutela dei dati personali degli interessati, individuando (*ex* art. 31 del Codice) ulteriori idonei accorgimenti volti a prevenire la conoscibilità dei dati da parte di terzi non autorizzati e la loro successiva utilizzabilità in operazioni di trattamento non compatibili con gli scopi che ne giustificano la raccolta (provv. 26 marzo 2015, n 181, doc. web n. 4002999);
- dichiarato illecito e vietato il trattamento dei dati personali idonei a rivelare lo stato di salute di un'interessata comunicati in via confidenziale dalla stessa a un proprio corrispondente operante presso un'agenzia affiliata ad un gruppo immobiliare e da quest'ultimo inoltrata a circa 200 agenzie appartenenti al medesimo gruppo. Dalla complessa istruttoria, effettuata anche mediante accertamenti ispettivi, è emerso che il trattamento di dati anche sensibili era stato effettuato in assenza di idonea informativa all'interessata e in violazione delle garanzie previste dall'art. 26 del Codice (provv. 23 aprile 2015, n. 242, doc. web n. 3966213);
- dichiarato illecito il trattamento effettuato mediante un sistema di videosorveglianza da un titolare del trattamento pubblico, in assenza dell'accordo con le rappresentanze sindacali e dell'autorizzazione del competente ufficio periferico del Ministero del lavoro, in violazione quindi degli artt. 114 del Codice e 4, l. n. 300/1970 (provv. 30 luglio 2015, n. 455, doc. web n. 4261028);
- disciplinato il trattamento di dati personali nell'ambito dei servizi di *mobile ticketing* prescrivendo: l'adozione di specifiche misure e accorgimenti per l'acquisto di titoli di viaggio digitali tramite ricorso al credito telefonico, con riguardo all'informativa e al consenso, alle misure di sicurezza e alla conservazione dei dati nonché l'adozione di ulteriori misure e accorgimenti per l'acquisto di titoli di viaggio digitali tramite ricorso alla carta di credito e ad un circuito di intermediazione (con provv. 10 settembre 2015, n. 467, doc. web n. 4273074 è stato posto in consultazione pubblica lo schema di provvedimento generale in materia);
- dichiarato illecito e vietato il trattamento di dati biometrici dei dipendenti di un ente locale effettuato in violazione dei princìpi di liceità, necessità, proporzionalità, pertinenza e non eccedenza dei trattamenti effettuati (art. 11, comma 1, lett. *a*) e *d*) del Codice), in assenza della previa notificazione

al Garante (art. 37 del Codice), nonché della preventiva richiesta di verifica preliminare (art. 17 del Codice) (provv. 22 ottobre 2015, n. 552, doc. web n. 4430740);

- prescritto ad un'Asl, oltre ad integrare il modello di informativa adottato, di incrementare le misure di sicurezza a protezione dei dati personali degli assistiti, provvedendo in particolare a: 1) mettere in atto specifici accorgimenti che consentano ai soli professionisti sanitari che hanno in cura il paziente di accedere al relativo *dossier* sanitario; 2) adottare specifici accorgimenti che consentano al personale amministrativo di accedere al *dossier* dei soli soggetti che sono coinvolti nell'attività amministrativa per la quale è necessario l'accesso e comunque con riferimento alle sole informazioni indispensabili per assolvere alle funzioni amministrative cui sono preposti (provv. 22 ottobre 2015, n. 550, doc. web n. 4449114).

In molti dei provvedimenti sopra citati l'Autorità, accertata la violazione di norme del Codice per le quali la legge prevede una sanzione amministrativa, ha avviato anche un procedimento sanzionatorio. In diversi casi inoltre il Garante, rilevando condotte punite come reato, ha disposto la trasmissione degli atti alla competente Procura della Repubblica.

21.5. *L'attività sanzionatoria del Garante*

21.5.1. Le violazioni penali e i procedimenti relativi alle misure minime di sicurezza

Nell'anno 2015, in relazione alle istruttorie effettuate, sono state inviate 33 segnalazioni di violazioni penali all'autorità giudiziaria (cfr. sez. IV, tab. 7) di cui:

- diciannove per la mancata adozione delle misure minime di sicurezza;
- sei per violazioni della l. n. 300/1970 (Statuto dei lavoratori), ora punite come reato dall'art. 171 del Codice;
- due per falsità nelle dichiarazioni e notificazioni al Garante;
- una per trattamento illecito dei dati;
- una per inosservanza di un provvedimento del Garante;
- quattro in relazione ad altre violazioni penali.

Come dimostrano i dati sopra riportati, permangono numerose le violazioni delle misure minime di sicurezza; ciò, nonostante si tratti di adempimenti di non particolare complessità, in vigore da più di dieci anni, che dovrebbero essere stati oramai "metabolizzati" sia dalle imprese che dagli enti pubblici. Deve essere nuovamente segnalata la ormai indifferibile esigenza di aggiornare il Disciplinare tecnico in materia di misure minime di sicurezza, All. B al Codice in vigore dal 2003, le cui prescrizioni appaiono in buona parte non più adeguate allo stato dell'evoluzione tecnica, anche alla luce della ormai consistente esperienza maturata dall'Autorità in sede di controllo. Tale revisione dovrebbe essere ispirata a criteri di semplificazione, rispetto ad adempimenti di natura prettamente burocratica oggi previsti dalle disposizioni, e di maggiore effettività delle misure, prevedendo adeguati accorgimenti tecnici che intervengano in modo progressivo in funzione della quantità e della qualità dei dati, nonché della complessità della struttura tecnologica utilizzata e del numero di incaricati che vi hanno accesso.

Al di là dei risvolti sanzionatori, occorre sottolineare che la mancata osservanza delle disposizioni relative alle misure minime di sicurezza è particolarmente grave perché espone, almeno potenzialmente, i dati personali degli interessati all'accesso da parte di persone non autorizzate e a trattamenti non consentiti, intaccando il naturale affidamento degli interessati nei confronti del titolare del trattamento.

Sotto il profilo procedurale, nel caso in cui venga rilevata una violazione di una o più delle misure minime di sicurezza (specificatamente previste dal Disciplinare tecnico sulle misure di sicurezza All. B al Codice), in base al disposto dell'art. 169, comma 2, del Codice, il Garante impartisce una prescrizione alla persona individuata come responsabile della predetta violazione e, successivamente, verificato il ripristino delle misure violate, ammette il destinatario della prescrizione al pagamento del quarto del massimo della sanzione prevista (pari a 30.000 euro). L'adempimento alla prescrizione ed il pagamento della somma vengono comunicati all'autorità giudiziaria competente per le valutazioni in ordine all'estinzione del reato.

In questo ambito merita una segnalazione la recente sentenza della Corte di Cassazione penale (n. 1986/2015) che ha respinto la questione di legittimità costituzionale relativa all'art. 169 del Codice, con riferimento agli artt. 2, 3, 21, 24, 25 della Costituzione. Nella motivazione si legge infatti che "non sussiste, infatti, alcun contrasto di tale disposizione con gli art. 3 e 24 Cost., perché rientra in generale nella piena discrezionalità del legislatore la fissazione dell'ammontare dell'oblazione ai fini dell'estinzione del reato, come avvenuto, attraverso il richiamo all'art. 162, comma 2-*bis*, in ragione di euro 30.000". Nella stessa sentenza la Suprema Corte afferma, con riferimento alla responsabilità penale che la stessa "è stata, del resto, positivamente accertata dalla Guardia di finanza nel corso delle indagini preliminari, attraverso l'accertamento diretto della mancata designazione dell'incaricato del trattamento in relazione ad un sito internet nel quale era possibile la raccolta di dati personali sensibili relativi a una serie indeterminata di persone", confermando la linea costantemente seguita negli anni dall'Autorità circa le conseguenze penali derivanti dall'omessa designazione degli incaricati del trattamento dei dati personali.

Come per l'anno precedente, anche nel 2015 si è avuta una rilevante incidenza dell'accertamento di violazioni penali relative allo Statuto dei lavoratori connesse, nella maggior parte dei casi, all'installazione di sistemi di videosorveglianza in assenza delle garanzie previste dall'art. 4, comma 2, l. n. 300/1970. Occorre tenere presente che la disciplina prevista dallo Statuto e relativa all'utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4) e al divieto di indagini sulle opinioni ai fini dell'assunzione (art. 8), costituisce ormai parte integrante delle disposizioni del Codice (artt. 113 e 114) ed è sanzionata dall'art. 171.

Sul punto appare opportuno evidenziare che tale disciplina ha subito profonde modifiche a seguito dell'adozione del d.lgs. 14 settembre 2015, n. 151 (cd. *Jobs Act*). Le modifiche apportate attengono sia alla parte sostanziale della disciplina del controllo a distanza dei lavoratori (art. 4, l. n. 300/1970) che a quella sanzionatoria (all'art. 171 del Codice).

In questo ambito, limitiamo la riflessione alle modifiche apportate alla parte sanzionatoria, ovvero alla nuova formulazione dell'art. 171 del Codice "La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della l. 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della l. n. 300 del 1970." Per quanto di interesse, la parte rilevante attiene al richiamo al primo e secondo comma dell'art. 4; tale norma prevede: al comma 1, che gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati, previo accordo sindacale o, in mancanza di accordo, previa autorizzazione della Direzione del lavoro; al comma 2, che la disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavora-

tore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

È venuto quindi meno il divieto dell'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Tale divieto, unitamente a quello relativo all'istallazione di sistemi che, pur avendo altre finalità, possano comportare anche il controllo a distanza dei lavoratori – in assenza dell'accordo sindacale o dell'autorizzazione dell'ispettorato del lavoro – costituivano, fino alla recente riforma, le condotte coperte dalla sanzione penale.

Ne consegue che la prima fattispecie, che puniva *tout court* l'istallazione di sistemi per finalità di controllo a distanza dell'attività dei lavoratori, è venura meno, mancando, nel nuovo testo, il suo presupposto (ovvero il divieto).

La sanzione penale resta invece con riferimento all'utilizzo di impianti audiovisivi e di altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, qualora installati in assenza dell'accordo sindacale o, in alternativa, dell'autorizzazione della Direzione territoriale del lavoro.

Meno chiara risulta invece l'inclusione del comma 2, dell'art. 4, dello Statuto nell'area coperta dalla sanzione penale prevista dal nuovo art. 171; tale comma sottrae, dall'ambito di applicazione delle disposizioni di cui al comma 1 (e quindi esonera dalla necessità di accordo/autorizzazione), gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze". Da ciò ne dovrebbe derivare che, ove il datore di lavoro ritenga erroneamente che determinati strumenti siano esonerati dagli adempimenti del primo comma (accordo o autorizzazione), verrebbe meno l'eccezione e quindi rientrerebbero nuovamente nella regola prevista dal comma 1, con la conseguenza che la condotta punita sarebbe, anche in questi casi, l'assenza dell'accordo o dell'autorizzazione. Sul punto occorrerà attendere l'applicazione della norma in sede penale.

È invece sicuramente sottratto alla valutazione del giudice penale il contenuto del comma 3 dell'art. 4 che prevede che "le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196".

Da ciò ne deriva che la mancata informazione ai lavoratori circa le modalità di uso degli strumenti e di effettuazione dei controlli rientra invece nell'orbita delle valutazioni di competenza dal punto di vista della legittimità del trattamento dei dati personali.

21.5.2. Le sanzioni amministrative

Nell'anno 2015 sono stati avviati n. 1.696 nuovi procedimenti sanzionatori amministrativi (cfr. sez. IV, tab. 6).

All'accertamento delle violazioni amministrative previste dal Codice può procedere:

- il personale dell'Ufficio addetto all'attività ispettiva a cui, sulla base di quanto previsto dall'art. 156, comma 9, del Codice, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, è attribuita la qualifica di ufficiale o agente di polizia giudiziaria;
- chiunque rivesta, nell'esercizio delle proprie funzioni, la qualifica di ufficiale o agente di polizia giudiziaria, in base a quanto previsto dall'art. 13, l. 24 novembte 1981, n. 689.

L'articolo 13 della l. n. 689/81 prevede: "Gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro possono, per l'accertamento delle violazioni di rispettiva competenza, assumere informazioni e procedere a ispezioni di cose e di luoghi diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica... All'accertamento delle violazioni punite con la sanzione amministrativa del pagamento di una somma di denaro possono procedere anche gli ufficiali e gli agenti di polizia giudiziaria".

I procedimenti sanzionatori iniziano, pertanto, con la contestazione in relazione ad istruttorie effettuate direttamente dall'Autorità ma anche sulla base di accertamenti effettuati autonomamente da corpi dello Stato quali la Guardia di finanza, i Carabinieri, la Polizia di Srato ecc. che possono accertare le violazioni amministrative in materia di protezione dei dati personali in occasione di attività svolte sulla base dei propri poteri, anche di polizia giudiziaria. Questo "doppio binario" risulta complessivamente efficace, considerata l'amplissima platea di soggetti tenuti all'osservanza delle regole previste dal Codice, che renderebbe velleitario un sistema di accertamento delle violazioni accentrato solo nell'Autorità.

L'assicurazione di una uniformità di giudizio e di interpretazione è peraltro assicurata, in quanto la legge affida invece al solo Garante il compito dell'applicazione delle sanzioni in tutti i casi nei quali, a seguito dell'accertamento, il contravventore, non avvalendosi della possibilità di definire il procedimento con il pagamento entro sessanta giorni dalla notifica del doppio del minimo della sanzione, decida di proseguire il procedimento medesimo inviando scritti difensivi o chiedendo l'audizione. In tutti questi casi è infatti l'Autorità a prendere la decisione finale circa l'applicazione della sanzione adottando l'atto finale dell'ordinanza ingiunzione, quantificandone l'importo, o l'archiviazione.

Le violazioni in relazione alle quali sono stati avviati procedimenti sanzionatori nel 2015 hanno riguardato:

- l'omessa o inidonea informativa – art. 161 (n. 223);
- il trattamento illecito amministrativo – art. 162, comma 2-*bis* (n. 1.350);
- l'utilizzo illecito dei dati delle persone iscritte al Registro pubblico delle opposizioni per finalità di *marketing* – art. 162, comma 2-*quater* (n. 5);
- l'omessa o incompleta notificazione – art. 163 (n. 44);
- l'omessa adozione delle misure minime di sicurezza di cui all'art. 33 del Codice – art. 162, comma 2-*bis* (n. 21);
- la conservazione di dati di traffico telefonico e telematico per un tempo superiore a quello srabilito dall'art. 132 del Codice – art. 162-*bis* (n. 9);
- l'omessa informazione o esibizione al Garante – art. 164 (n. 28);
- l'inosservanza di un provvedimento del Garante – art. 162, comma 2-*ter* (n. 10);
- la violazione di disposizioni del Codice in relazione a banche dati di particolari rilevanza o dimensioni – art. 164-*bis*, comma 2 (n. 6).

Un approfondimento merita il dato relativo alle 1.350 violazioni di cui all'art. 162, comma 2-*bis* che si è definito "trattamento illecito amministrativo". La disposizione prevede una sanzione pecuniaria, da 10.000 a 120.000 euro in relazione alla violazione delle disposizioni di cui all'art. 167. Quest'ultima disposizione, a sua volta, richiama numerose disposizioni del Codice, estremamente eterogenee, e, in particolare, gli artt: 17 (verifica preliminare), 18, 19, 20, 21, 22, commi 8 e 11 (disposizioni concernenti il trattamento dei dati da parte di soggetti pubblici), 23, 25, 26, 27 (disposizioni concernenti il trattamento dei dati da parte dei soggetti privati), 45 (trasferimenti all'estero vietati), 123, 126, 129 e 130 (disposizioni specifi-

che per le comunicazioni elettroniche). Nel 2015 le violazioni concernenti il "trattamento illecito amministrativo" accertate hanno riguardato:

- in 1.270 casi, la violazione del consenso dell'interessato in rapporto agli artt. 23 e 130 del Codice. In particolare, occorre evidenziare che è stata effettuata, grazie alla collaborazione con la Guardia di finanza, un'attività straordinaria nei confronti dei soggetti operanti nel settore del *money transfer*, che ha condotto alla contestazione di n. 1.172 violazioni nei confronti delle società coinvolte. Dagli accertamenti è emerso che tali società utilizzavano illecitamente i dati di centinaia di persone o clienti ignari per frazionare fittiziamente il trasferimento all'estero di ingenti somme di denaro ed eludere così i limiti che impongono agli operatori la segnalazione, agli enti preposti per i controlli antiriciclaggio, di transazioni monetarie al di sopra di certe soglie (cfr. *newsletter* del Garante n. 406, 28 settembre 2015 doc. web n. 4277760);
- in 38 casi, violazioni commesse da enti pubblici (nella maggior parte dei casi comunicazioni o diffusioni di dati personali comuni senza i necessari presupposti di legge o regolamento);
- in 5 casi, violazioni delle misure e degli accorgimenti prescritti dal Garante nell'ambito di una verifica preliminare sulla base dell'art. 17 del Codice;
- in 18 casi, violazioni commesse da enti pubblici con riferimento a dati sensibili o giudiziari;
- in 3 casi, violazioni commesse da fornitori di reti pubbliche di comunicazione o di servizi di comunicazione elettronica con riferimento ai dati di traffico di abbonati o utenti;
- in 5 casi, violazioni commesse da soggetti privati o pubblici in relazione alle ulteriori garanzie previste dall'art. 26 del Codice per il trattamento di dati sensibili;
- in 15 casi, violazioni commesse da fornitori di reti pubbliche di comunicazione o di servizi di comunicazione elettronica con riferimento all'effettuazione di comunicazioni indesiderate.

Analizzando i dati statistici sopra riportati si può rilevare che:

- in senso assoluto, per l'anno di riferimento, il numero di violazioni accertate in merito all'obbligo di fornire all'interessato tutte le informazioni sul trattamento dei dati, non è srata la violazione più ricorrente, a differenza che negli anni precedenti;
- la violazione maggiormente riscontrata è risultata quella relativa alla mancata acquisizione del consenso degli interessati; sono state riscontrate in merito quasi 1.300 violazioni, in parte legate all'effettuazione di comunicazione indesiderate, mentre, per larghissima maggioranza, le stesse sono state riscontrate, come accennato, nell'ambito di una vasta operazione condotta dalla magistrarura nei confronti di alcune società di *money transfer* che utilizzavano i dati personali di clienti inconsapevoli.

I procedimenti sanzionatori definiri nell'anno 2015 con provvedimento di ordinanza adottato dall'Autorità, relativamente a violazioni contestate negli anni precedenti al 2015 e non definite all'epoca attraverso il pagamento spontaneo in misura ridotta da parte del contravventore, sono stati 386. Di questi, 294 hanno comportato l'applicazione di una sanzione (per un ammontare complessivo di somme ingiunte pari a 3.013.000 euro) e 92 si sono invece conclusi con l'archiviazione in quanto la parte ha potuto dimostrare nel procedimento di non aver commesso la violazione contestata o che la violazione non era ad essa imputabile.

Tra le ordinanze adottate, quelle più significative, sotto il profilo della rilevanza degli aspetti giuridici, sono brevemente riassunte di seguito.

- Applicabilità delle tutele del Codice nei casi di comunicazioni indesiderate effettuate nei confronti di persone giuridiche. Nel caso in cui i trattamenti di dati personali effettuati dal titolare siano riconducibili all'ambito di applicazione di quelli previsti dall'art. 130, comma 1, del Codice, ai fini dell'attribuzione della responsabilità dell'illecito amministrativo derivante dalla disapplicazione dell'istituto del consenso, non si può fare riferimento alla definizione di interessato di cui all'art. 4, comma 1, lett. *i*) del Codice (i.e, "persona fisica cui si riferiscono i dati personali") bensì a quella di "contraente" prevista dall'art. 4, comma 2, lett. *f*), del Codice, che include anche le persone giuridiche. Ne discende che, nelle ipotesi di cui al cit. art. 130, comma 1, la tutela del dato personale ricomprende anche la persona giuridica-contraente e che la mancata acquisizione del consenso della stessa al trattamento configura una violazione del Codice (ordinanza-ingiunzione 7 maggio 2015, n. 276, doc. web n. 4207931).
- Deroga del Codice al principio di personalità di cui agli artt. 2 e 3, l. n. 689/1981. Riguardo il principio di personalità di cui agli artt. 2, 3 e 7, l. n. 689/1981, si evidenzia come la disciplina dettata dal Codice costituisca *lex specialis* rispetto alle previsioni della predetta legge, in quanto quest'ultima risulta essere una fonte di pari grado, richiamabile, per effetto dell'art. 166 del Codice, solo "in quanto applicabile". Il Codice dispone che gli adempimenti siano posti in essere, in primo luogo, dal titolare del trattamento, che, secondo quanto previsto all'art. 28 del Codice – quando il trattamento è effettuato da una persona giuridica, da una p.a. o da un qualsiasi altro ente, associazione od organismo – risulta essere "l'entità nel suo complesso", ferma restando la facoltà in capo allo stesso, nell'ambito del potere di organizzazione del trattamento dei dati, di delegare l'assolvimento di taluni adempimenti anche a persone (fisiche o giuridiche) individuate, ai sensi dell'art. 29 del Codice, quali responsabili del trattamento (ordinanza-ingiunzione 29 gennaio 2015, n. 51, doc. web n. 3925407).
- Ambito di applicazione dell'art. 13, comma 5-*bis* del Codice. Quando l'invio dei *curricula* avviene a fronte della pubblicazione di inserzioni su quotidiani e periodici di annunci ed offerte di lavoro, tale invio non può essere considerato spontaneo ai sensi dell'art. 13, comma 5-*bis* del Codice, bensì sollecitato dal titolare del trattamento, come, peraltro, esplicitato nel parere del Garante del 10 gennaio 2002, e quindi sottoposto agli obblighi previsti dal Codice, con particolare riferimento all'informativa agli interessati (ordinanza-ingiunzione 5 marzo 2015, n. 132, doc. web n. 3999100).
- Ambito di definizione del titolare del trattamento. L'operazione di pubblicazione in elenco telefonico di numerazioni mobili, benché effettuata dal *dealer* in fase di attivazione delle sim, deve essere imputata all'operatore telefonico, in qualità di titolare del trattamento. Ciò vale aldilà della formale qualifica di titolare del trattamento, attribuita al *dealer* nel contratto stipulato con l'operatore telefonico. Infatti, i poteri previsti dal Codice per l'esercizio della titolarità comprende, in primo luogo, quello relativo "[al]le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati" (artt. 4, comma 1, lett. *f*) e 28 del Codice). Nel caso specifico, avendo l'operatore telefonico adottato autonomamente ogni determinazione in ordine alla predisposizione dei moduli e della contrattualistica da presentare ai clienti per le attivazioni telefoniche, il *dealer* è obbligato a seguire dettagliatamente le istruzioni impartite e ad attenersi alle indicazioni operative di volta in volta decise proprio dall'operatore

telefonico (ordinanza-ingiunzione 18 giugno 2015, n. 362, doc. web n. 4253116).

- Rapporto tra titolare e responsabile del trattamento. A fronte di un'attività di polizia giudiziaria, nell'ambito della quale sono state individuate delle responsabilità penali in capo a un funzionario e al direttore di una filiale bancaria per aver attivato due conti correnti all'insaputa dell'interessato, il Garante ha stabilito che, sotto il profilo della protezione dei dati personali, le responsabilità connesse agli adempimenti in materia di informativa e consenso devono, nel caso di specie, essere imputate alla banca che, in qualità di titolare del trattamento, adotta ogni decisione in merito alle finalità e alle modalità del ttattamento, agli strumenti utilizzati, anche "sotto il profilo della sicurezza". Pertanto, anche in presenza delle designazioni dei direttoti di filiali e dei funzionari quali responsabili e/o incaticati del trattamento, ai sensi degli artt. 29 e 30 del Codice, la responsabilità per i fatti oggetto di contestazione va individuata in capo alla banca che ha omesso di vigilare sull'osservanza delle proprie istruzioni (ordinanza-ingiunzione 11 giugno 2015, n. 348 doc. web n. 4243123).

L'ammontare dei pagamenti effettivamente effettuati nell'anno 2015 da parte dei soggetti nei cui confronti sono srati avviati procedimenti sanzionatoti amministrativi è risultato complessivamente pati a 3.345.515 euro (cfr. sez. IV, tab. 8) di cui:

- 1.647.468 euro, pagati a titolo di definizione in via breve;
- 1.170.930 euto, a seguito di ordinanze-ingiunzione adottate dal Garante in tutti i casi in cui la parte non si è avvalsa della facoltà di definizione in via breve di cui al punto precedente;
- 270.000 euro, per la definizione, in sede amministtativa, dei procedimenti relativi alla mancata adozione delle misure minime di sicurezza;
- 257.117 euro, quali ulterioti entrate derivanti dall'attività sanzionatotia (es. riscossione coattiva).

Gli importi relativi alle sanzioni applicate dal Garante sono versati sul bilancio dello Stato. Sulla base di quanto previsto dall'art. 166 del Codice, tali proventi, nella misura del 50% del totale annuo sono riassegnati al fondo stanziato per le spese di funzionamento dell'Autorità previsto dall'art. 156, comma 10, del Codice e utilizzabili unicamente per l'esercizio della artività ispetriva e di divulgazione della disciplina della protezione dei dati personali.

22 Le relazioni comunitarie e internazionali

Nel 2015, è proseguita l'intensa attività del Garante a livello europeo ed internazionale (cfr. sez IV, tab. n. 20).

Nell'ambito della modernizzazione degli strumenti normativi in materia di protezione dei dati personali si è giunti alla conclusione dell'*iter* legislativo europeo per la definizione del cd. pacchetto protezione dati, che si compone di una proposta di regolamento, volta a disciplinare i trattamenti di dati personali sia nel settore privato sia nel settore pubblico e destinata a sostituire la direttiva 95/46/CE, e di una proposta di direttiva indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali, che sostituirà ed integrerà la decisione quadro 977/2008/GAI (che l'Italia non ha ancora attuato).

La riforma presenta diverse novità e comporta un ripensamento dell'intera architettura normativa ed organizzativa della protezione dati (per un quadro sinterico dei due strumenti, con particolare attenzione alle novità introdotte rispetto all'attuale quadro normativo, v. par. 22.1).

Il 2015 è stato anche contrassegnato dagli importanti contributi della CGUE volti a chiarire il quadro applicativo della disciplina in materia di protezione dei dati. Di particolare rilevanza è stata la sentenza del 6 ottobre 2015 (causa C-362/14; cd. caso Schrems), nella quale la Corte ha dichiarato l'invalidità della decisione 2000/520/CE della Commissione del 26 luglio 2000 che aveva attestato che gli Stati Uniti, attraverso il cd. *Safe Harbor* (sistema per il trasferimento dei dati verso gli USA, applicabile alle sole imprese che lo sottoscrivono), garantiscono un adeguato livello di protezione dei dati personali trasferiti.

La vicenda all'origine del giudizio della CGUE inizia nel giugno del 2013, quando uno studente di giurisprudenza austriaco chiede all'autorità di protezione dei dati irlandese di ordinare a Facebook di sospendere il trasferimento dei dati personali dei propri utenti europei negli Stati Uniti, che – a seguito delle rivelazioni di Snowden – non potevano considerarsi in grado di garantire adeguatamente il rispetto del diritto alla protezione dei dati e della vita privata. La Corte di giustizia, investita della questione pregiudiziale dall'Alta Corte di giustizia irlandese, ha in primo luogo reputato che l'esistenza di una decisione della Commissione che dichiara che un Paese terzo garantisce un livello di protezione adeguato non può sopprimere né ridurre i poteri delle autorità nazionali di controllo: queste ultime devono anzi poter esaminare, in piena indipendenza, se il trasferimento rispetti i requisiti della direttiva e, in caso ritengano che la decisione della Commissione sia invalida, rivolgersi ai giudizi nazionali affinché questi ultimi possano rinviare la causa dinanzi alla Corte di giustizia.

La sentenza ha inoltre ritenuto che nella suddetta decisione la Commissione ha omesso di effettuare una valutazione circa l'adeguatezza del sistema legislativo statunitense e degli impegni internazionalmente assunti (essa infatti non menziona l'esistenza, negli Stati Uniti, di norme intese a limitare le ingerenze da parte di autorità pubbliche che vadano oltre quanto previsto in una società democratica, né l'esistenza di una tutela giuridica efficace contro tali ingerenze), limitandosi invece ad esaminare il regime del *Safe Harbor*, applicabile alle sole imprese che lo sottoscrivono e non alle autorità pubbliche. Secondo la Corte una normativa che consenta alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comu-

nicazioni elettroniche deve essere considerata lesiva del diritto fondamentale al rispetto della vita privara. Nella valurazione d'adeguatezza è inoltre di cruciale importanza il riconoscimento di una tutela giurisdizionale effettiva.

La decisione della Corte è stara al centro di un'intensa attività del Gruppo Art. 29 volta ad approfondite i riflessi della sentenza sul piano nazionale ed europeo anche al fine di costituire una posizione comune delle autorirà per una sua corretta applicazione (v. par. 22.3).

22.1. *La riforma del quadro giuridico europeo in materia di protezione dei dati*

L'*iter* legislativo europeo che ha portato alla definizione del cd. pacchetto protezione dati composto dal regolamento generale sulla protezione dei dati e dalla direttiva sulla protezione dati nelle attività giudiziarie e di polizia è stato particolarmente lungo e faticoso.

Parlamento europeo e Consiglio UE, che partecipano su un piano paritario alla procedura di co-legislazione (definita "ordinaria" in base al TFUE), hanno presentato in questi anni numerosi emendamenti ai testi proposti dalla Commissione. Diversi sono stati anche i contributi sottoposti all'attenzione dei legislatori dal Gruppo Art. 29, che ha licenziato numerosi pareri e documenti sia sull'intera riforma sia su singole tematiche (v. *infra*), e dal Garante europeo per la protezione dei dari.

Il Parlamento europeo aveva concluso la prima lettura il 12 marzo 2014, votando su entrambi i testi, mentre l'esame da parte del Consiglio UE (gruppo di lavoro DAPIX) è srato molto più lungo e complesso, tanto che l'adozione in prima lettura da parte del Consiglio "Giustizia e affari interni" si è avuta solo nel giugno 2015 per la proposta di regolamento e nell'ottobre 2015 per la proposta di direttiva. Sono stati successivamente ed immediatamente avviati i cd. "triloghi" interistituzionali (Parlamento-Consiglio-Commissione) nei quali la Presidenza di turno del Consiglio UE ed i relatori del Parlamento europeo, assistiti dalla Commissione, hanno esaminato i punti di divergenza e individuato possibili testi di compromesso per i due strumenti. Tali testi sono stati infine approvati per il Consiglio dal COREPER il 16 dicembre, e il 17 dicembre per il Parlamento dalla competente Commissione LIBE (Libertà dei cittadini e diritti fondamentali) che ha accettato il testo votaro dal COREPER il giorno precedente, cosicché il Consiglio ha ratificato l'accordo politico con il voto definitivo del COREPER del 18 dicembre. L'*iter* legislativo si è concluso il 14 aprile 2016 con l'approvazione senza modifiche da parte del Parlamento UE di entrambi i testi in seconda lettura e con la formale presa d'atto del Consiglio UE in data 21 aprile 2016 (la pubblicazione è prevista sulla GUUE del 4 maggio 2016).

Sul piano dei contenuti, numerose sono le novità introdotte dai due strumenti rispetto all'esistente quadro normativo. Questo ha infatti indotto a prevedere un periodo di due anni ai fini dell'applicazione del regolamento dopo la sua entrata in vigore (con la pubblicazione sulla GUUE); identico periodo è previsto per la trasposizione della direttiva da parte dei legislatori nazionali, fissato in 2 anni dalla dara di pubblicazione, in modo che entrambi gli strumenti siano applicati contemporaneamente dagli Stati dell'Unione. Si può dunque affermare che l'orizzonte temporale di completamento della cd. fase discendente della riforma si collochi nella primavera-estate del 2018.

Regolamento UE protezione dati

Riguardo al regolamento, il testo si articola su 11 Capi, con 99 articoli e 173 "considerando". L'impianto concettuale e giuridico dell'attuale direttiva 95/46/CE (che sarà abrogata alla data di applicazione del regolamento) trova sostanziale conferma. I princìpi fondamentali del trattamento (qualità dei dati, presupposti di liceità), i diritti degli interessati (in particolare, informativa e accesso, consenso, ret-

tifica e opposizione), l'esistenza di autorità incaricate specificamente di garantire il rispetto della normativa restano pilastri essenziali anche nella riforma, trovando peraltro fondamento negli artt. 7 ed 8 della Carta dei diritti fondamentali dell'UE. Il regolamento dà tuttavia ulteriore enfasi ad alcuni di tali elementi e introduce, per altro verso, componenti innovative, di cui si danno nel prosieguo le linee essenziali.

Diritti degli interessati:

- potenziamento dei contenuti obbligatori dell'informativa (con possibilità per i titolari di ricorrere ad icone o forme grafiche di informativa in associazione all'informativa testuale vera e propria);
- introduzione del diritto ad una cancellazione estesa dei propri dati personali (oblio), comprendente anche copie o *link* riferiti a tali dati, ma non incondizionata, essendo previste limitazioni all'esercizio del diritto per contemperare altre esigenze e interessi legittimi (libertà di espressione, interesse pubblico, finalità archivistiche nel pubblico interesse);
- introduzione della possibilità di chiedere la "limitazione" del trattamento (anziché la cancellazione), ad esempio in attesa di definire l'esattezza o obsolescenza di un dato o per continuare ad utilizzare il dato per specifiche finalità, in particolare giudiziarie;
- introduzione del diritto alla portabilità dei dati (riferito ai dati forniti direttamente dall'interessato, sulla base del consenso o di disposizioni contrattuali), con alcune eccezioni, in particolare per i dati contenuti in archivi di interesse pubblico;
- previsione di una forma di consenso rafforzato (non solo "inequivocabile", ma anche "esplicito") qualora vi si ricorra per legittimare il trattamento di dati sensibili;
- definizione di condizioni restrittive (intervento obbligatorio dei soggetti che detengono la potestà genitoriale) ai fini della valida prestazione del consenso da parte di minori in rapporto all'offerta di "servizi della società dell'informazione"; la soglia di età relativa alla minorità è fissata fra i 13 ed i 16 anni, e la scelta in merito è rimessa al legislatore nazionale.

Obblighi dei titolari di trattamento:

- introduzione del cd. "approccio basato sul rischio" e, più in generale, del principio di *accountability* ovvero di responsabilizzazione dei titolari di trattamento. Ciò si traduce in una ampia serie di disposizioni che tendono a promuovere approcci proattivi, e non reattivi, in un'ottica di prevenzione di possibili problematiche e di riduzione degli oneri considerati puramente burocratici, quali la notifica dei trattamenti. Ricordiamo le principali:

a) applicazione dei princìpi di *privacy by design* e *privacy by default* in via generale;
b) obbligo per tutti i titolari/responsabili di condurre una valutazione di impatto prima di procedere ad un (nuovo) trattamento, seguita eventualmente dalla consultazione dell'Autorità di controllo qualora il titolare non ritenga sufficienti le misure di mitigazione del rischio a lui note o disponibili;
c) introduzione e disciplina della figura del "Responsabile della protezione dati" (ovvero il *Data Protection Officer*), la cui nomina è obbligatoria per i soggetti pubblici, mentre è facoltativa per i soggetti privati ad eccezione di alcuni trattamenti particolarmente a rischio e salva diversa disposizione della legislazione nazionale. Il regolamento fissa i requisiti essenziali in termini di indipendenza, conoscenze e compiti del DPO;
d) disciplina specifica della contitolarità di trattamento e della ripartizione di

responsabilità fra contitolari, e specificazione del vincolo di natura contrattuale che deve sussistere fra titolare e responsabile del trattamento;

e) eliminazione dell'obbligo di notifica dei trattamenti all'Autorità (sostituita dall'obbligo di tenuta di documentazione sui trattamenti svolti, a disposizione dell'Autorità);

f) introduzione dell'obbligo generalizzato per tutti i titolari di notificare eventuali violazioni di dati personali (*personal data breach*), all'Autorità ed agli interessati, secondo un criterio di rischio più o meno elevato per i diritti dell'interessato stesso;

g) potenziamento del ricorso a codici deontologici (anche settoriali) e introduzione dell'istituto della certificazione dei trattamenti, entrambi utilizzabili anche ai fini di trasferimenti di dati in Paesi terzi; in questo contesto, il regolamento assegna alle Autorirà di conrrollo un ruolo non esclusivo di monitoraggio dell'attuazione e del rispetto di codici deontologici e schemi di certificazione, lasciando spazio anche a soggetti privati a ciò abilitati o accreditati.

Governance della protezione dari:

- definizioni dettagliate di ruolo e poteri delle Autorità nazionali di controllo (discendenti direttamente dal regolamento e non dal diritto nazionale);
- previsione di veri e propri obblighi di cooperazione fra Autorità nazionali con possibilità di svolgere ispezioni e indagini congiunte sul rispettivo territorio nazionale;
- in contesti di trattamento di natura multinazionale, introduzione del meccanismo dello "spottello unico" per i titolari/responsabili di trattamento (salva la competenza esclusiva dell'Autorità nazionale per trattamenti svolti da soggetti pubblici nazionali) e del "meccanismo di coerenza".

a) Ciò si concretizza nella previsione della figura della "Autorità capofila", sostanzialmente l'Autorità competente sullo stabilimento principale (o unico) del titolare/responsabile nell'UE; a tale Autorità è rimessa la decisione ultima (ad es., per quanto riguarda l'adozione di codici deontologici, clausole contrattuali, *Binding corporate rules*, o la composizione di contenziosi) anche se attraverso un processo di codecisione cui partecipano tutte le altre Autorità "interessate" a vario titolo nell'UE. Vi è poi una riserva di competenza dell'Autorità nazionale (non capofila) rispetro a "reclami" che si dimostrino avere carattere esclusivamente nazionale, e quindi risultino privi di ripercussioni su altri Stati membri; in caso di controversie fra, in particolare, l'Autorità capofila e le altre Autorità interessate, interviene il Comitato europeo della protezione dei dati con funzione dirimenre;

b) definizione di funzioni, poteri e ruolo del "Comitato europeo della protezione dei dati" quale garante di coerenza e armonizzazione. Tale Comitato è l'erede dell'attuale Gruppo Art. 29, formato da rappresentanti delle Autorità di controllo nell'UE, ma le sue caratteristiche ne travalicano considerevolmente gli ambiti. Si tratta infatti di un soggetto dotato di personalità giuridica, con una presidenza ed un segretariato permanente, incaricato di redigere e diffondere Linee guida, direttive, pareri su molteplici aspetri sostanziali e procedurali del regolamento, e avente il ruolo di decisore ultimo vincolante in caso di controversie fra Autorità nella trattazione di casi gestiti secondo il meccanismo di coerenza e/o attraverso il meccanismo dello "sportello unico" (codecisione uniforme);

c) definizione di un sistema unificato europeo di sanzioni amministrarive

(pecuniarie) che le Autorità di controllo hanno il potere di comminare in aggiunta a o in sostituzione dei provvedimenti assunti in base ai poteri loro conferiti dal regolamento. Tali sanzioni sono distribuite secondo tre diversi livelli di gravità delle violazioni (con importi pecuniari rispettivamente fissati in termini di massimo edittale); nel testo del regolamento sono indicati specifici criteri (attenuanti/aggravanti) per la definizione della gravità della violazione da parte delle Autorità di controllo, suscettibili di integrazioni ad opera del Comitato europeo della protezione dei dati.

In termini generali, altri elementi importanti da segnalare:

- campo di applicazione territoriale e materiale del regolamento: ai fini dell'applicazione delle disposizioni contenute nel regolamento, viene meno il criterio di collegamento basato sull'utilizzo di "strumenti" situati nel territorio UE da parte di titolari non stabiliti in un Paese UE (Art. 4(1)c della direttiva 95/46; art. 5, comma (2) del Codice italiano), poiché si introduce il criterio del *targeting* (offerta di prodotti o servizi destinati a soggetti presenti nell'UE). Tale disposizione mira a garantire che le tutele offerte dalla legislazione UE trovino applicazione ai dati oggetto di trattamento *tout court*, senza riguardo, quindi, a fattori di natura materiale. La tutela in questione non riguarda solo i "cittadini" dell'UE, ma, appunto, chiunque si trovi nell'UE e sia destinatario di tali prodotti o servizi (in conformità degli artt. 7 e 8 della Carta dei diritti fondamentali).
- Previsione di un margine di flessibilità lasciato agli Stati membri per alcune tipologie di trattamento, in particolare i trattamenti svolti per finalità di "pubblico interesse" o "in adempimento di un obbligo legale" nonché per i trattamenti di cui al Capo IX (giornalismo, lavoro, ricerca scientifica, statistica, storica, archivi). Si tratta di un elemento piuttosto peculiare in uno strumento, quale il regolamento, la cui *ratio* consiste proprio nel superare divergenze e differenze legate al diritto nazionale; purtuttavia, l'introduzione di questi ampi margini di flessibilità trova giustificazione nell'esistenza di un quadro molto articolato di norme nazionali che, soprattutto in alcuni settori e in alcuni Paesi (fra cui il nostro), già contengono numerose salvaguardie per la tutela dei dati personali e costituiscono uno sviluppo importante oltre che il frutto dell'esperienza applicativa raccolta in questi ultimi venti anni. Negli ambiti sopra ricordati, gli Stati membri sono pertanto autorizzati a "introdurre o mantenere" disposizioni di diritto nazionale che consentano di "adattare" quelle contenute nel regolamento. Tale rinvio espresso al legislatore nazionale è accompagnato da un elenco dei requisiti sostanziali che devono essere soddisfatti da ogni misura legislativa nazionale cui si ricorra in questi settori: specificazione delle finalità perseguite; dimostrazione della necessità del trattamento; specificazione ulteriore delle condizioni generali di liceità; indicazione delle tipologie di dati oggetto di trattamento, degli interessati e dei destinatari eventuali dei dati; previsioni sui periodi di conservazione; norme sostanziali e procedurali per garantire, in particolare, liceità e correttezza dei trattamenti in questione.
- Occorre rilevare, inoltre, che il regolamento fa rinvio al legislatore nazionale con riguardo a ulteriori tipologie di trattamento: in particolare in ambito sanitario e rispetto ai trattamenti di dati genetici o biometrici (con possibilità di prevedere condizioni o limitazioni ulteriori); quanto ai criteri di nomina di un DPO, ampliabili ai sensi del diritto nazionale; rispetto alla possibilità di richiedere autorizzazioni da parte dell'Autorità di controllo per taluni trattamenti a rischio; con riguardo alle norme che devono disciplinare

istituzione e componenti delle Autorità di controllo ed alla possibile previsione di sanzioni, anche penali, ulteriori rispetto a quelle contenute nel regolamento. D'altro canto, si deve ricordare che il regolamento prevede espressamenre, come già la direttiva 95/46 al suo art. 13, la possibilità di introdurre con legge nazionale deroghe ai diritti degli interessati per specifiche finalità (interesse pubblico, sicurezza pubblica, sicurezza dello Stato, salute pubblica, ecc.), purché tali deroghe siano necessarie e proporzionate e, in particolare, rispettino l'"essenza" del diritto alla protezione dei dati. Significativamente, quest'ultima condizione riflette il linguaggio utilizzato dalla CGUE nella richiamata sentenza sulla tutela offerta in Paesi terzi ai dati trasferiti dall'UE (Causa C-362/14, Facebook c. Schrems, v. par. 22.3). Tale possibilità è prevista anche rispetto ai trattamenti per finalità scientifiche, statistiche, storiche, archivistiche nel pubblico interesse, salve le garanzie che il diritto nazionale deve prevedere, in particolare, l'esistenza di misure atte a favorire l'applicazione del principio di "minimizzazione dei dati".

- Un cenno specifico merita anche la materia dei trasfetimenti di dati personali verso Paesi terzi. In via generale, il regolamenro mantiene inalterati i presupposti fissati dalla direttiva 95/46: si prevede un divieto generale di trasferimento verso Paesi terzi od organismi internazionali, salva l'esistenza di una decisione di adeguatezza assunta dalla Commissione con riguardo a singoli Paesi ovvero a settori di trattamento o organismi internazionali; in assenza di una decisione del genere, è data la possibilità di ricorrere a garanzie conttattuali o ad altri presupposti in deroga, quali il consenso dell'inreressato o la prestazione contrattuale. Tuttavia, da un lato vengono irrigiditi i requisiti di adeguatezza attraverso l'obbligo per la Commissione di effettuare una valutazione complessiva, che tenga conto dell'intero quadro normativo nel Paese terzo e, quindi, anche delle tutele offerte in caso di trattamenti per finalità di polizia e giustizia e, più in generale, delle tutele esistenti rispetto ai diritti fondamentali di cui alla Carta. Per altro verso, vengono introdotte disposizioni specifiche che disciplinano l'uso di clausole contrattuali modello, norme vincolanti di impresa (Bcr) ed altre autorizzazioni di trasferimento *ad hoc* concesse dalle singole Autorità nazionali (necessariamente con intervento del "meccanismo di coerenza"). Vi è inoltre una disposizione, fortemente voluta dal Parlamento eutopeo, con cui si vietano i trasferimenti richiesti da autorità giudiziarie o amministrative di Paesi terzi qualora essi non trovino fondamento in accordi internazionali di mutua assistenza giudiziaria o in strumenti analoghi, di natura bilaterale o multilaterale.

Direttiva polizia e giustizia

Il testo della direttiva si articola in X Capi, 65 arricoli, 107 "considerando". L'impianto è sostanzialmente e strutturalmente allineato al regolamento di cui mantiene immutata l'articolazione in Capi e la corrispondenza dei titoli. I princìpi fondamentali del trattamento (liceità e correttezza, qualità dei dati, presupposti di liceità), i diritti degli interessati (in particolare, informativa e accesso, consenso, rettifica e opposizione), l'esistenza di autorità incaricate specificamente di garantire il rispetto della normativa restano pilastri essenziali anche nella direttiva, ancorché con differenze rispetto a quanto previsto dal regolamento dovute al particolare ambito disciplinato. Al riguardo va infatti considerato che – pur nell'affermazione del diritto fondamentale alla protezione dei dati, contenuta nell'art. 16 del TFUE, che costituisce peraltro la base giuridica individuata dalla Commissione per entrambi gli strumenti – la Dichiarazione 21 insisteva sulla necessità di norme specifiche per la cooperazione penale e di polizia. È per questo che, in assenza di un quadro armo-

nizzato dei princìpi di protezione dati nello specifico settore dovuta alla non completa integrazione sviluppata al riguardo, il riferimento normativo più vicino fosse alla decisione quadro n. 977 del 2008, che dettava regole sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale. È così che il tenore delle disposizioni è in parte ispirato a quelle della decisione quadro, che viene contestualmente abrogata con l'entrata in vigore della direttiva. La direttiva si pone quindi come *lex specialis* rispetto al regolamento per i trattamenti rientranti nel suo campo di applicazione. Sarà pertanto molto importante definire esattamente l'articolazione con le disposizioni del regolamento e gli ambiti di rispettiva applicazione (ad es., per le attività svolte nei settori dell'asilo, immigrazione, disciplina degli stranieri).

Il campo di applicazione materiale copre i trattamenti svolti dalle autorità competenti in base al diritto nazionale per finalità di prevenzione, indagine, accertamento e perseguimento di reati, inclusa la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica.

Le autorità competenti possono a loro volta essere sia autorità pubbliche sia qualsiasi altro organismo o entità incaricato dal diritto nazionale di esercitare l'autorità pubblica e i poteri pubblici nel settore su ricordato.

Riguardo agli aspetti più salienti, va innanzi tutto dato atto che la direttiva costituisce il primo strumento che detta regole armonizzate per i trattamenti di dati svolti dagli Stati membri nel settore "polizia e giustizia", creando vincoli certi per i legislatori nazionali, verificabili dalla Commissione e dalla stessa Corte di giustizia.

La direttiva lascia agli Stati membri la possibilità di prevedere garanzie più elevate: si tratta di un aspetto importante per la salvaguardia dei diritti fondamentali, considerando che la discussione avutasi in Consiglio ha portato ad una riscrittura in particolare degli articoli relativi ai diritti degli interessati che, prevedendo un maggior numero di deroghe, rischia di comprimere l'effettivo esercizio dei diritti di informazione, accesso, rettifica, cancellazione dei dati. Questo lascia un margine di manovra ampio agli Srati nel definire le categorie di trattamenti, il relativo rischio e le conseguenti regole. La direttiva prevede infatri che sia data una informazione molto generale sul trattamento, similmente a quanto previsto dal Codice all'art. 53, e che il legislatore individui i casi in cui debbano essere fornite informazioni più dettagliate, ciò al fine di salvaguardare le indagini ed altri aspetti di rilevante interesse pubblico. La direttiva prevede inoltre che laddove i dati personali siano trattati nell'ambito di una indagine giudiziaria penale, il legislatore debba disciplinare il modo in cui tali diritti possano essere azionabili.

Anche per quanto riguarda il trattamento dei dati sensibili – allineandosi con la decisione quadro – non c'è nella direttiva un divieto di trattamento con specificazione delle eccezioni, ma la previsione che il trattamento possa essere effettuato solo se strettamente necessatio ed in presenza di adeguate garanzie.

Relativamente agli obblighi di titolari e responsabili si segnala l'attenzione posta sulla necessità di introdurre misure di sicurezza adeguate ai rischi del trattamento. La stessa direttiva prescrive le misure da adottare in caso di trattamenti automatizzati e le elenca.

Regole simili a quelle introdotte dal regolamento vigono pet la cooperazione con l'Autorità di controllo e la definizione dei casi in cui è obbligatoria la consultazione preventiva di derta Autorità (per la notifica del *data breach*, per la tenuta dei registri e dei *log* delle operazioni).

La direttiva prevede inoltre l'obbligo di designare un "responsabile per la protezione dei dati" da parte delle autorità competenti e ne disciplina figura, compiti e risorse, indicando che può essere anche designato un unico responsabile per più

autorità competenti, tenuto conto della loro sttuttura organizzativa e dimensioni. Per quanto concerne il trasferimento di dati verso autorità competenti in Paesi terzi o otganizzazioni internazionali, le disposizioni sono allineate a quelle del regolamento per quanto concerne l'accettazione di un sistema generale basato sull'adeguatezza del Paese/organizzazione, anche se un margine più ampio è lasciato ai ttasferimenti in deroga, che comunque non devono mai essete ripetitivi o massivi. Anche gli accordi bilaterali già in vigore tra Stati UE e Paesi terzi restano tali finché non modificati. È stato inserito un articolo che, pur prevedendo una serie di stringenti condizioni, consente il trasferimento di dati personali dalle autorità competenti a soggetti privati in Paesi terzi, laddove necessario per le indagini.

I compiti ed i poteri delle Autorità di controllo sono riragliate sullo schema del regolamento, riconoscendo la tripartizione dei poteri in potere d'indagine, correttivo e consultivo effettivo, ma nella direttiva il riferimento alle attività da svolgere è molto più sintetico, ancora una volta lasciandosi spazio al legislatore nazionale.

La cooperazione delle Autorità di controllo si svolge attraverso il Comirato europeo istituito dal regolamento, cui partecipano le autorità designate dal legislatore nazionale per sorvegliare l'applicazione dei trattamenti di dati svolti nei settori ricadenti nella direttiva.

È stata inoltre inserita una disposizione che chiede al legislatore nazionale di disporre che le autorità competenti mettano in opera meccanismi efficaci per incoraggiare la segnalazione riservata di violazioni della direttiva.

22.2. *Le conferenze delle autorità su scala internazionale*

La Conferenza internazionale delle autorità di protezione dati

La 37ª Conferenza internazionale, che rappresenta 110 autorità di protezione dei dati del mondo ed esperti del settore, si è tenuta ad Amsterdam dal 26 al 29 ottobre 2015. Come negli anni precedenti, la Conferenza si è articolata in una sessione aperta, occasione di scambio con i diversi *stakeholder* sui temi di protezione dati e una sessione riservata alle sole Autorità.

Nella sessione chiusa della Conferenza sono stare presentate e adottate quattro Risoluzioni. La prima, sul tema degli accessi, da parte di autorità pubbliche, ai dati personali in possesso di società commerciali, evidenzia la necessità che sia le entità private cui le autorità si rivolgono, sia i governi adottino adeguate politiche per garantire trasparenza (cd. *transparency reporting*), in particolare sulle tipologie di richiesta e la loro base giuridica (doc. web n. 4810449).

La seconda risoluzione, sul tema *privacy* e azione umanitaria internazionale, sottolinea la necessità di garantire anche in questo settore il pieno rispetto dei princìpi di protezione dati (doc. web n. 4810431). La terza risoluzione, che è invece dedicata alla attività di cooperazione con il relatore speciale USA su diritto alla *privacy*, mira a sollecitare governi e altri attori coinvolti ad offrire il supporto necessario al relatore per adempiere alle sue funzioni (doc. web n. 4810415). Una quarta risoluzione riguarda infine la direzione strategica della Conferenza, per il periodo 2016-18 (doc. web n. 4810405).

È stata inoltre approvata una dichiarazione contenente due comunicati, rispettivamente sul tema dei dati genetici e sulla protezione dei dati nell'ambito della sicurezza e della *intelligence* (doc. web n. 4814854).

Nella sessione aperta è srato presentato il progetto *Privacy bridges*, su iniziativa dell'autorità olandese e predisposto dall'Università di Amsterdam e dal Massachusetts *Institute of Technology* di Cambridge (MA, USA), nel quale sono delineate diverse proposte per la risoluzione dei contrasti nella tutela della *privacy* e dei

dati personali tra il sistema europeo e quello statunitense. Le questioni e le 10 proposte contenute nel *Report Privacy Bridges* (doc. web n. 4814871) sono state l'oggetto principale della discussione nella sessione aperta della Conferenza.

Sempre nella sessione aperta, il Garante ha presentato la propria esperienza di cooperazione internazionale avviata con l'Albania nell'ambito dell'evento organizzato dal GPEN ("GPEN *Meeting:* 2016 *and beyond – A New Era in Global Enforcement Cooperation*") ed è stata parte attiva del *panel* "*Data Stewardship for a 21st Century Data-Driven World*", organizzato dall'*Accountability Foundation*, in particolare sul tema *big data.*

La Conferenza (attraverso il suo Comitato esecutivo) pubblica una *newsletter* per informare regolarmente in merito alle attività svolte.

La Conferenza di primavera, che riunisce le autorità di protezione dei dati personali europee si è tenuta a Manchester dal 18 al 20 maggio 2015.

La Conferenza delle autorità europee (*Spring Conference*)

Quest'anno la Conferenza dal titolo "*Navigating the Digital Future – let's get practical!*", si è concentrata sul tema dei diritti degli interessati, in particolare sugli strumenti pratici e le strategie da porre in essere per facilitarne l'esercizio, ivi compreso il rafforzamento del ruolo delle autorità di protezione dei dati nell'applicazione della normativa e delle forme di cooperazione tra le stesse autorità a livello europeo.

Nel corso della Conferenza sono state adottate tre diverse risoluzioni.

Una prima risoluzione mira a promuovere un ruolo sempre più attivo delle autorità di protezione dati per rispondere alle crescenti aspettative di tutela nel futuro digitale e richiama la necessità che le autorità di protezione dei dati siano dotate di risorse sufficienti a svolgere il loro ruolo istituzionale (doc. web n. 4810039).

La seconda risoluzione si propone invece di facilitare la cooperazione tra le stesse autorità in particolare con la predisposizione di una piattaforma web destinata a raccogliere materiali e risoluzioni della Conferenza (doc. web n. 4810056).

Con l'ultima risoluzione l'Andorra è stata accreditata tra i membri della *Spring Conference* secondo i criteri previsti dalle Linee guida per l'ammissione adottare il 23 aprile 2004 alla Conferenza di Rotterdam.

22.3. *La cooperazione tra autorità garanti nell'UE: il Gruppo Art. 29*

La prosecuzione a ritmi serrati dei lavori relativi al pacchetto europeo di riforma in materia di protezione dei dati e alcuni recenti interventi della Corte di giustizia sul tema hanno richiesto, nel 2015, una maggiore flessibilità nell'agenda delle autorità garanti nell'UE riunite nel Gruppo Art. 29. Il Gruppo (attraverso i lavori dei suoi sottogruppi e le sei riunioni plenarie tenutesi nel 2015) ha così continuato a fornire indicazioni e approfondimenti atttaverso i pareri adottati sulla base dei temi strategici fissati nel programma di lavoro relativo al biennio 2014-2015 adottato il 3 dicembre 2013 (doc. web n. 3815727). Le autorità hanno anche colto ogni possibile occasione per contribuire alla creazione di un nuovo quadro giuridico più coerente, garantista ed efficace – inviando proprie osservazioni alle tre istituzioni europee impegnate nel trilogo (v. *infra*) – e per chiarire gli effetti sull'attuale quadro normativo delle significative sentenze adottate dalla CGUE in materia di conservazione dei dati di traffico (v. sentenza Digital Rights Ireland Ltd., doc. web n. 3845166), legge applicabile (sentenze Google Spain, doc. web n. 3127044, e Weltimmo, doc. web n. 4810583) e trasferimenti di dati all'estero (sentenza Schrems, doc. web n. 4810595).

Le ripercussioni di quest'ultima sentenza (v. anche par. 22) sono state oggetto di una particolare attenzione da parte del Gruppo che – oltre ad impegnare nella sua

analisi vari sottogruppi – vi ha dedicato una sessione speciale della Plenaria tenutasi il 15 ottobre 2015. All'esito di tale plenaria, il Gruppo ha adottato una dichiarazione (doc. web n. 4810342) nella quale, oltre a dare prime indicazioni in ordine agli aspetti relativi al trasferimento di dati verso gli Stati Uniti (v. *infra*), ha anche messo in luce l'assoluta necessità di adottare una posizione comune nell'applicazione della sentenza, sottolineato come la sorveglianza massiva e indiscriminata, punto centrale della decisione della Corte, sia incompatibile con il quadro europeo, e ribadito la necessità che le istituzioni europee e gli stati membri aprano un dialogo con gli Stati Uniti per il raggiungimento di soluzioni giuridiche volte a garantire che il trasferimento dei dati oltreoceano avvenga nel rispetto dei diritti fondamentali.

Concetti chiave della direttiva – Revisione parere legge applicabile

Come anticipato, il Gruppo ha continuato ad occuparsi, nel corso dell'anno, anche di un'altra rilevante sentenza della CGUE, la sentenza del 14 maggio 2014, caso Google Spain (doc. web n. 3127044) che ha riconosciuto in capo alla società statunitense la titolarità del trattamento dei dati personali che appaiono nell'elenco dei risultati del suo motore di ricerca e l'applicabilità della disciplina europea (nel caso specifico spagnola) in materia di protezione dei dati. Con il documento del 16 dicembre 2015 (WP 179, doc. web n. 4810638) il Gruppo ha infatti aggiornato il precedente parere 8/2010 sulla individuazione della normativa applicabile in materia di protezione dei dati alla luce delle indicazioni della Corte. Il documento si è concentrato sulla parte della sentenza che ha interpretato la nozione di stabilimento prevista dall'art. 4, paragrafo 1, lettera *a*), della direttiva 95/46 e, richiamando anche la sentenza Weltimmo (doc. web n. 4810583), ha chiarito che, tra i trattamenti effettuati "nel contesto delle attività di uno stabilimento" del titolare nel territorio di uno Stato membro, rientrano anche quelli posti in essere, in un altro Stato membro, da una succursale o una filiale che svolga attività "inestricabilmente connesse" al trattamento di dati personali in questione (come tali, nel caso di Google Spain, sono considerare, ad es., il trattamento dei dati da parte di Google e la raccolta pubblicitaria effettuata dagli stabilimenti di Google in UE). Al fine di individuare la legge applicabile (o le leggi applicabili) sarà quindi necessario verificare, in ciascun caso, se le attività svolte da uno o più stabilimenti di uno stesso titolare siano "inestricabilmente connesse" al trattamento dei dati effettuato dal medesimo titolare.

Il pacchetto di riforma UE

Con riferimento al nuovo quadro posto in essere dal pacchetto di riforma sulla protezione dei dati, il Gruppo è varie volte intervenuto fornendo il proprio contributo tecnico nelle diverse fasi del processo normativo.

Rivolgendosi ai diversi interlocutori politici coinvolti nella riforma, il Gruppo (lettere 17 giugno 2015, doc. web n. 4810133) ha richiamato l'attenzione su una serie di priorità ed obiettivi da considerare nell'elaborazione dei nuovi strumenti. Secondo il Gruppo occorreva *in primis* che il pacchetto di riforma consentisse di mantenere alto il livello di protezione fino ad ora garantito dalla direttiva 95/46 e che non rappresentasse in nessun modo un ridimensionamento del sistema di tutela esistente. Riguardo ai rapporti tra i due strumenti in discussione – regolamento e direttiva sulla protezione dei dati nelle attività di contrasto – occorreva che piena coerenza fosse garantita tra i due quadri normativi, e che la proposta di direttiva rappresentasse un'eccezione ai principi del regolamento limitata esclusivamente al settore del *law enforcement* per la prevenzione e perseguimento dei reati, senza estendersi ad altre attività di autorità pubbliche. Con riferimento ai principi chiave della riforma, il Gruppo ha sottolineato che il concetto di dato personale doveva essere ampio a sufficienza da rispondere alle esigenze di protezione derivanti dalle nuove tecnologie. Occorreva inoltre una stretta osservanza del principio di finalità – che non ammette trattamenti incompatibili con gli scopi legittimi del trattamento originario – e che fossero garantiti gli strumenti necessari ad assicurare un agevole eser-

cizio dei diritti da parte degli interessati, in un quadro normativo fondato su una nuova *governance* basata sulla prossimità agli individui e sull'efficienza per il mondo delle imprese.

A tal fine, alcuni suggerimenti tecnici sono stati offerti dal Gruppo in vista del trilogo nel documento che figura in allegato alle citate lettere (doc. web n. 4810122).

Sempre con riferimento al pacchetto di riforma, il Gruppo, con una lettera del 25 settembre 2015 indirizzata alle tre istituzioni europee, ha fornito diverse osservazioni riguardo alla struttura interna del Comitato europeo della protezione dei dati (utili alla discussione nel trilogo ma anche alle future regole procedurali dello stesso Comitato) affinché tale organo abbia una struttura flessibile ed equilibrata, in grado di valorizzare la rete decentralizzata delle autorità di protezione dei dati e di fornire un efficiente e stabile coordinamento (doc. web nn. 4810318 e 4810328).

Aerei a pilotaggio remoto (RPAS)

Con riferimento alla protezione dei dati nel settore delle nuove tecnologie, il Gruppo ha portato a conclusione il lavoro di approfondimento iniziato nel 2014 su impulso della Commissione (v. Relazione 2014, p. 175) sugli aerei a pilotaggio remoto, cd. droni, per scopi civili (ivi comprese le attività di *law enforcement*). Con l'adozione del parere 1/2015 (WP231, doc. web n. 4810724) il Gruppo ha fornito indicazioni – distinguendo tra oneri e raccomandazioni per gli operatori – per consentire un utilizzo di tali mezzi rispettoso dei principi di protezione dei dati. Riguardo agli obblighi per gli operatori, il parere sottolinea la necessità di verificare la liceità del trattamento e di individuare la corretta base giuridica, di rispettare l'obbligo di fornire un'adeguata informativa tenendo conto delle peculiarità delle operazioni svolte, di osservare i principi di minimizzazione, proporzionalità e finalità del trattamento e di adottare idonee misure di sicurezza. Tra le raccomandazioni rivolte agli *stakeholder*, il parere pone invece l'accento sull'opportunità di introdurre e/o rafforzare un quadro giuridico che consenta l'utilizzo dei droni nel rispetto di tutti i diritti fondamentali, di individuare modalità di cooperazione tra autorità di protezione dei dati e autorità per l'aviazione civile in modo da richiamare l'attenzione degli operatori al rispetto delle regole in materia di protezione dei dati, di utilizzare fondi di ricerca UE per l'individuazione di strumenti tecnologicamente adeguati volti a fornire l'informativa agli interessati e favorire l'identificazione dei droni. Infine, il parere si rivolge anche a costruttori e operatori: raccomandando l'approntamento di misure di *privacy by default*, la promozione di codici deontologici, l'adozione di misure per rendere il più possibile visibile e identificabile un drone.

Le implicazioni dell'uso civile dei droni su *privacy* e protezione dei dati sono state oggetto anche di una conferenza internazionale organizzata dall'autorità ungherese (Budapest, 5-6 febbraio 2015) nella quale esperti di *privacy*, rappresentanti governativi, società civile, operatori commerciali e accademici si sono confrontati sui principi necessari a garantire un uso responsabile di tali dispositivi, nel rispetto dei diritti delle persone.

Cloud computing

Sempre nell'ambito delle nuove tecnologie con l'adozione del parere 2/2015 (WP232, doc. web n. 4810737) il Gruppo ha portato a termine il lavoro di analisi del codice di condotta europeo sul *cloud computing* predisposto dal gruppo di rappresentanti dell'industria *Cloud Select Industry Group*-CSIG. Il parere, nel ricordare che l'adesione al codice non mette le società al riparo dall'attività di *enforcement* delle autorità di protezione dei dati, si sofferma sul sistema di *governance* (che, tra l'altro, dovrà essere più stringente, attento ai cambiamenti nel quadro legislativo europeo e non prevedere la partecipazione del Gruppo Art. 29) e sulla necessità di fornire informazioni ai clienti sul luogo dove i dati verranno conservati e sulle eventuali richieste di accesso agli stessi provenienti da autorità di *law enforcement* di Paesi

terzi. Il Codice, inoltre, dovrà contenere un chiaro richiamo alla definizione di dato personale della normativa europea (ed eventualmente citare la pseudonimizzazione solo come misura di sicurezza), prevedere specifici scenari nei casi di trattamenti di dati sensibili e un regime più chiaro per l'allocazione delle responsabilità che non sia sfavorevole al cliente (titolare del trattamento). A quest'ultimo dovrà essere riconosciuto il diritto di *audit*, almeno attraverso la predisposizione da parte del fornitore del servizio *cloud di Key Performance Indicators* (KPI) e con questi il fornitore del servizio (responsabile del trattamento) dovrà cooperare per fornire all'interessato l'informativa di cui all'art. 10 e riconoscere all'interessato il diritto alla portabilità dei dati (anticipando, in questo, il regolamento).

Cookie Sweep

Il 3 febbraio 2015 è stato adottato il Rapporto dei garanti europei sull'impiego di *cookies* nell'utilizzo della rete (WP229, doc. web n. 4810673). Il Rapporto rappresenta il documento conclusivo di un'analisi congiunta (*cookie sweep*) articolata in due diverse fasi: una verifica statistica dei *cookie* utilizzati in rete e delle loro caratteristiche e una più approfondita analisi dei meccanismi di informativa e consenso in uso. Dall'esame effettuato dalle aurorità è emerso che nonostante molti operatori informino gli utenti della presenza di cookie, ancora non è frequente la raccolta di un valido consenso per il telativo trattamento dei dati, così come previsto dalla direttiva *e-Privacy* e in linea con le precisazioni finora fornite dal Gruppo Art. 29 (cfr. WP194, doc. web n. 2439391 e WP208, doc. web n. 2982826).

Dati relativi alla salute nel contesto *m-Health*

A seguito dell'adozione da parte della Commissione europea del Libro verde in materia di *Mobile Health* e per rispondere ad una specifica richiesta della stessa Commissione intesa ad ottenere un chiarimento sulla definizione di dato relativo alla salute utilizzata nel contesto delle *apps* relative a stili di vita e *well-being*, il Gruppo ha inviato una lettera alla DG-*Connect* fornendo indicazioni e chiari esempi per identificare e trattare i dati relativi alla salute anche nel contesto delle nuove tecnologie (doc. web nn. 4810096 e 4810086). Il testo distingue sostanzialmente tra tre categorie di dati raccolti attraverso tali tipologie di *app*: 1. i dati chiaramente relativi alla salute (ad es., quelli utilizzati in un contesto medico); 2. una categoria di dati che, a seconda del contesto, possono qualificarsi come dati relativi alla salute (in particolare, i dati che, seppure neutri di per sé, sono trattati per tirare conclusioni sullo stato di salute attuale o futuro); 3. esempi di dati che non costituiscono dati relativi alla salute (ad es., il dato relativo ai passi effettuati, singolarmente trattato).

Borders, Travel e Law Enforcement

Il Gruppo ha lavorato intensamente sulle implicazioni della direttiva concernente la tutela delle persone fisiche con tiguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (v. par. 22.1). Con il parere 3/2015 (WP233, doc. web n. 4810751) il Gruppo, partendo dal testo adottato dal Consiglio nel setrembre 2015, esprime perplessità su alcuni aspetti critici e formula suggerimenti. In particolare, il parere sottolinea la necessità di tener adeguatamente conto nel testo del fatto che il diritto alla protezione dei dati personali ha il rango di diritto fondamentale che va declinato orizzontalmente nelle varie disposizioni della direttiva in modo da garantire un livello elevato di tutela (la raccomandazione 87(15) adottata dal Comitato dei ministri del Consiglio d'Europa rappresenta al riguardo il minimo comune denominarore da garantire da parte del legislatore dell'UE). Il documento ribadisce la necessità di assicurare coerenza tra regolamento e direttiva quanto meno sui punti essenziali del disegno normativo. Quanto agli aspetti specifici, il parere considera negarivamente l'allargamento dell'ambito di applicazione materiale della direttiva volto a coprire anche la prevenzione di rischi per la sicurezza pubblica, preferendo al riguardo il testo originale della Commissione.

Sottolinea inoltre l'importanza che la direttiva collochi la correttezza del trattamento tra i suoi princìpi chiave.

Quanto al principio di finalità, il documento richiama l'attenzione sulla necessità di garantire una idonea base legale per ogni ulteriore finalità del trattamento – non incompatibile – rispetto a quella originaria. Si chiede, inoltre, di inserire nuovamente nel testo dell'articolato la necessità di tener distinte le varie categorie di soggetti cui i dati si riferiscono (sospetti, non sospetti, vittime, testimoni, ecc.) e di ridefinire il trattamento dei dati sensibili (cui vanno aggiunti i dati biometrici) sulla base del principio del divieto come regola, prevedendo poi le eccezioni. Si chiede inoltre di specificare che la profilazione non può avvenire a partire dai dati sensibili. Quanto ai diritti dell'interessato il documento chiede il ripristino di diverse garanzie esistenti nel testo iniziale della Commissione, anche per quanto concerne il trattamento di dati di minori. Ulteriori osservazioni sono formulate riguardo ai poteri delle Autorità di protezione dati, la sicurezza del trattamento dei dati, gli obblighi del titolare, l'informazione in caso di *data breach*, il trasferimento di dati verso Paesi terzi.

Il Gruppo ha inoltre lavorato alla preparazione di una dichiarazione sulle conseguenze della sentenza della CGUE dell'8 aprile 2014 che ha annullato la direttiva sulla conservazione dei dati di traffico (direttiva *data retention*). La bozza di dichiarazione è stata predisposta dal Garante e dai colleghi della Repubblica ceca, soffermandosi soprattutto sulla necessità di un'applicazione uniforme delle legislazione di protezione dei dati, in particolare con riferimento ai tempi di conservazioni dei dari, e alle Linee guida su come garantire che l'accesso delle autorità di *law enforcement* sia selettivo e non massiccio ed indiscriminato. Il lavoro svolto è alla fine confluito in un questionario predisposto dal Garante volto ad ottenere informazioni sulla situazione negli Stati membri, al fine di acquisire elementi sui regimi di *data retention* esistenti nei vari Paesi e valutare quale sia stato l'impatto su di essi della sentenza della CGUE.

Sempre riguardo alla conservazione dei dati, si evidenzia che l'Alta Corte di giustizia del Regno Unito ha bocciato, il 17 luglio, la legge adottata, in via d'urgenza nel 2014 (*Data Retention and Investigatory Powers Act* – DRIPA). La Corte ha ritenuto che la stessa non forniva regole precise e chiare per assicurare che ai dati si potesse avere accesso, solo con l'autorizzazione di un giudice o di un'autorità indipendente, al fine di prevenire e accertare "*serious offences*" e per i soli casi strettamente necessari.

In tema di *cybercrime*, il Gruppo ha adottato ed inviato una lettera al Comitato per la Convenzione sul *cybercrime* (T-CY) del Consiglio d'Europa in occasione della Conferenza sul *cybercrime* (17-19 giugno, Strasburgo): la lettera, nel ricordare che in Europa trovano applicazione, per i trattamenti per finalità di *law enforcement* la direttiva 95/46 (anche se con le deroghe di cui all'art. 13 della stessa), la Convenzione 108/1981, la raccomandazione 87(15) e la decisione quadro 2008/977, richiama l'attenzione sulla necessità di rispettare sempre il principio di liceità del trattamento, di non considerare mai il consenso dell'interessato come idoneo presupposto per legittimare i trattamenti per finalità di *law enforcement* ed analizza i 18 scenari prospettati alla scorsa Conferenza sul *cybercrime*, fornendo, ove possibile, alcune specifiche indicazioni (doc. web nn. 4814829 e 4814840).

È inoltre proseguita l'attività su PNR, con la predisposizione di una lettera contenente i commenti del Gruppo Art. 29 sullo stato del negoziato relativo alla proposta di un PNR europeo e il rapporto presentato dal relatore al Parlamento europeo adottata il 19 marzo. Si è inoltre tenuto un seminario il 18 marzo organizzato dalla Commissione europea in cui si sono confrontati rappresentanti delle Autorità di protezione dati e dei governi che beneficiano dei finanziamenti per progetti PNR

nazionali. Il Gruppo ha anche incontrato gli esponenti delle compagnie aeree europee riuniti nell'AEA (SAS, *AirFrance, British Airways, Lufthansa, Austrian Airlines, Brussels Airlnes,* KLM, IATA) per rappresentare i timori delle compagnie riguardo alle richieste di dati PNR del governo messicano che, dal 1° aprile ha previsto importanti sanzioni ai vettori europei per mancato trasferimento di dati PNR.

In tema di TFTP (*Terrorist Finance Tracking Programme*), il Gruppo ha anche adottato (23 marzo) ed inviato una lettera alle istituzioni comunitarie per chiedere che le DPA siano coinvolte sulla rinegoziazione dell'Accordo TFTP (doc. web n. 4814901). La lettera tiene anche conto delle osservazioni formulate dal Garante per l'ACC Europol.

Inoltre, il Gruppo ha iniziato ad esaminare il tema delle intercettazioni dei cavi transatlantici e il Garante ha partecipato il 30 luglio alla prima riunione (tenutasi all'Aja) del gruppo ristretto di *drafting* (composto da rappresentanti di diversi sottogruppi del WP29) al fine di predisporre una bozza di indice per un parere in materia.

Cooperation

Nell'ottica di intensificare la cooperazione tra le Autorità di protezione dati, il Gruppo di lavoro ha cominciato a dedicare parte di attività ad incontri e *workshop* mirati ad anticipare parte del futuro lavoro derivante dai nuovi obblighi previsti dalla proposta di regolamento UE di protezione dati (assistenza reciproca, sportello unico, meccanismo di coerenza, ecc.). In particolare, si è tenuto a Budapest presso l'Autorità ungherese il 17 e 18 novembre un *workshop* avente ad oggetto la redazione di un unico e condiviso modulo di "ricorso" da utilizzare per i casi transfrontalieri in cui è necessaria una cooperazione ed assistenza tra le Autorità. È stata condivisa l'opportunità di redigere un unico modulo da utilizzare sia nel periodo transitorio che sotto il nuovo regolamento e di creare una piattaforma dedicata per lo scambio di informazioni fra le Autorità. È emerso il problema della lingua (e relativi costi) da utilizzare per la cooperazione (un accordo generale è stato espresso sulla lingua inglese) ed il problema della tempistica e delle diverse divergenze nazionali sui tempi per la decisione.

Come risultato del *workshop*, il Gruppo ha elaborato una prima bozza di modulo per la cooperazione su ricorso.

Protezione dei dati in ambito finanziario

È stata intensa l'attività del Gruppo riguardo alle tematiche di protezione dei dati in ambito finanziario, in particolare con la prosecuzione da parte del Garante, su mandato della Plenaria, del coordinamento del sottogruppo *Financial matters*.

Il Gruppo ha continuato ad occuparsi dello scambio automatizzato di dati a fini fiscali, un fenomeno in crescente espansione sia a livello internazionale (v. i *common reporting standard* dell'OCSE che si propongono quale modello globale per lo scambio di informazioni tra amministrazioni fiscali ai fini della lotta all'evasione internazionale), sia a livello europeo, in particolare con la direttiva 2014/107 (recante modifica della direttiva 2011/16/UE per quanto riguarda lo scambio automatico obbligatorio di informazioni nel settore fiscale) che ha sostanzialmente recepito il modello OCSE dei CRS in ambito europeo (v. Relazione 2014, p. 177).

Tale tema è stato oggetto della dichiarazione del Gruppo del 4 febbraio 2015 (WP230, doc. web n. 4810708), rivolta ai governi nazionali e alle istituzioni comunitarie competenti affinché gli accordi bilaterali e multilaterali che prevedono scambi automatizzati di dati a fini fiscali, nonché le relative normative nazionali, assicurino adeguate garanzie per la protezione dei dati senza portare a raccolte e scambi massivi, non proporzionati allo scopo perseguito.

Il Gruppo ha quindi predisposto e adottato un questionario sullo scambio automatizzato di dati a fini fiscali, rivolto alle aurorità nazionali competenti. Attraverso il questionario sono state raccolte informazioni sul livello di implementazione da parte dei diversi Stati membri degli obblighi, introdotti a livello europeo ed inter-

nazionale, di scambio-dati nell'ambito della lotta all'evasione fiscale. Le risposte pervenute hanno costituito una base informativa su cui è stato fondato il lavoro di elaborazione di specifiche Linee guida (WP234, doc. web n. 4810763) indirizzate ai governi affinché i princìpi di protezione dei dati siano tenuti in dovuta considerazione nei relativi accordi (bilaterali e multilaterali) che prevedano lo scambio di informazioni per il contrasto all'evasione fiscale. La redazione del testo delle *Guidelines* è stata curata dal Garante e dall'EDPS (*co-rapporteur*), anche alla luce del confronto avuto con esperti della Commissione europea (DG TAXUD) che, nel supportare il lavoro del Gruppo, hanno suggerito di dividere le Linee guida in raccomandazioni per Stati membri e raccomandazioni per Paesi terzi. Le Linee guida forniscono indicazioni circa le garanzie di protezione dei dati da applicare in tre diversi casi: (i) nello scambio di dati personali tra gli Stati membri dell'UE; (ii) nello scambio di dati personali tra uno Stato membro dell'UE e un Paese terzo che è stato oggetto di una decisione di adeguatezza della Commissione europea, e (iii) nello scambio di dati personali tra uno Stato membro UE e un Paese terzo che non è stato oggetto di una decisione di adeguarezza della Commissione europea. Vengono inoltre identificate diverse garanzie che dovrebbero essere sempre inserite nel contesto dello scambio automatico di dati per il contrasto all'evasione fiscale.

Sempre in tema di lotta all'evasione fiscale, il Gruppo ha avanzato un'esplicita richiesta in merito allo stato di ratifica dell'Accordo FATCA (*Foreign Account Tax Compliance Act,* la legislazione USA anti evasione fiscale *off shore*) nei vari Stati membri (cfr. par. 4.6). Il Garante ha raccolto e analizzato i contributi pervenuti dalle diverse delegazioni. Le informazioni raccolte mostrano che la maggior parte dei Paesi ha firmato (e poi recepito nella legislazione nazionale) l'Accordo tra il proprio governo e il governo degli USA al fine di migliorare la *compliance* fiscale e applicare la normativa FATCA. Solo in un caso, uno Stato membro ha firmato l'Accordo che però non è ancora in vigore. In altri casi, l'Accordo FATCA è stato firmato ed è entrato in vigore senza la necessità di una proceduta di ratifica in base alla loro legislazione nazionale. È opportuno sottolineare che alcuni Stati membri prevedono di firmare Accordi di attuazione del FATCA il più presto possibile. In base all'analisi delle risposte il Gruppo discuterà gli ulteriori passi da intraprendere (ad es., la possibile valutazione della qualità delle misure di recepimento – se presenti – in base al diritto nazionale dal punto di vista della protezione dei dati, nonché il coordinamento delle azioni di *enforcement* sulle norme di attuazione di FATCA).

Nel 2105, il Gruppo ha altresì portato avanti l'analisi delle normative cd. MIFID2 (pacchetto composto dalla direttiva 2014/65 relativa ai mercati degli strumenti finanziari e dal regolamento 600/2014, cd. MIFIR) e MAR (*Market Abuse Regulation*: regolamento 596/2014 relativo all'abuso di informazioni privilegiate e la manipolazione del mercato). Durante un incontro con esperti della Commissione europea (DG FISMA), per entrambi gli strumenti normativi sono emersi alcuni punti di criticità sui seguenti aspetti: a) obblighi di registrazione di telefonate e comunicazioni elettroniche da parte delle società di investimento per consentire alle autorità competenti di svolgere i loro compiti di supervisione per un corretto andamento del mercato; b) *whistleblowing*; 3) pubblicazione delle sanzioni e, con specifico riferimento a MAR: 4) prevenzione e rilevazione dell'abuso di mercato e 5) le cd. *insider lists*. Dalla discussione è emersa altresì la necessità che nell'effettiva implementazione dei princìpi *privacy*, di cui si è occupata ESMA (*European Securities Markets Authority*) attraverso la predisposizione di *Technical standard*, occorrerebbe un intervento del Gruppo Art. 29 per declinare tali princìpi in termini più concreti. In proposito si è anche tenuto un incontro con ESMA che ha confermato le predette criticità. Di conseguenza il Gruppo ha adottato ed inviato una lettera alla

Commissione (DG FISMA) per evidenziare nuovamente gli aspetti problematici degli *standard* tecnici che ESMA ha elaborato (doc. web n. 4814764).

Infine, il Gruppo ha replicato alla lettera con cui l'*International Organisation of Securities Commissions* (IOSCO) ha risposto alla lettera adottata dal Gruppo il 18 settembre 2014 con la quale il WP29 aveva rilevato l'assenza di salvaguardie, sul piano della protezione dei dati, nel "*Multilateral Memorandum of Understanding concerning consultation and the exchange of information*" (MMoU), aperto alla firma delle autorità di vigilanza, per una migliore cooperazione nel settore dei valori mobiliari e volto ad assicurare il rispetto delle discipline interne in tale settore (doc. web n. 4814818).

Trasferimento dati all'estero

Il tema dell'accesso da parte di autorità pubbliche di Paesi terzi ai dati personali trasferiti all'estero attraverso gli strumenti previsti dagli artt. 25 e 26 della direttiva 95/46/CE e delle misure che devono essere adottate al fine di garantire il rispetto dei principi di necessità e proporzionalità anche nel caso in cui tali accessi siano effettuati sulla base delle deroghe previste per ragioni di giustizia o sicurezza pubblica è stato al centro dell'attività svolta, nel corso dell'anno, dal Gruppo attraverso il sottogruppo *International Transfers*.

Documento esplicativo sulle *Binding corporate rules for processor*

In particolare, l'argomento è stato affrontato nel documento esplicativo sulle *Binding corporate rules* per responsabili del trattamento (WP 204 rev. 01, doc. web n. 4810659) che ha modificato il precedente documento relativo alle *Bcr for processor* al fine di meglio chiarire i contenuti dell'obbligo di segnalazione alle DPA posto in capo ai *processor* (responsabili del trattamento) che ricevono una richiesta di *disclosure* da parte delle autorità di *law enforcement* o di pubblica sicurezza di un Paese terzo. Secondo le nuove indicazioni, le società dovranno comunicare alle DPA competenti tutte le informazioni disponibili in relazione alla richiesta ricevuta per consentire a queste ultime di valutare l'eventuale blocco o divieto di trasferimento ulteriore di dati; nel caso di divieti di comunicazione in ordine alla richiesta di *disclosure* ricevuta, le società dovranno cercare di adempiere all'obbligo, anche impugnando dinanzi alle corti competenti tali divieti. Nel caso in cui la preventiva informazione alle DPA risulti impossibile, le società dovranno fornire comunque, successivamente alla *disclosure*, informazioni sulle richieste ricevute (e, eventualmente, sulle ragioni per le quali non sia stato possibile informare prima la DPA).

Invalidità della decisione di adeguatezza del *Safe Harbour* e conseguenze

Lo stesso tema è stato discusso poi nel quadro di un'analisi avviata per verificare gli effetti della sentenza Schrems della CGUE – che ha invalidato la decisione 2000/250 con cui la Commissione europea aveva dichiarato adeguata la protezione offerta dal cd. "approdo sicuro" (v. *supra*) – non solo sulle decisioni di adeguatezza della legislazione di un Paese terzo, ma anche sugli altri strumenti di trasferimento dei dati all'estero previsti dall'art. 26 direttiva 95/46/CE (Clausole contrattuali *standard* adottate dalla Commissione europea, contratti *ad hoc*, *Binding corporate rules* e deroghe).

Al riguardo, il 16 ottobre, il Gruppo Art. 29 ha adottato uno *statement* (doc. web n. 4810342) con il quale ha anzitutto ribadito che, tenuto conto della sentenza, i dati personali non possono essere più trasferiti dall'UE agli USA sulla base del *Safe Harbour* e che pertanto, per porre in essere tali trasferimenti, si deve, allo stato, far riferimento alle deroghe previste dall'art. 26, par. 1 (da interpretare restrittivamente tenuto conto che si tratta appunto di "deroghe") e, soprattutto, agli strumenti di cui all'art. 26, par. 2 (clausole contrattuali *standard* e *ad hoc*, Bcr). Anche il ricorso a tali strumenti, tuttavia, dovrà essere attento: il titolare del trattamento deve infatti addurre comunque garanzie "adeguate" per i trasferimenti anche alla luce degli specifici elementi evidenziati dalla Corte (necessaria esistenza sia di rimedi giuridici che consentano all'interessaro di accedere a dati personali che lo riguardano, di ottenerne la rettifica o la soppressione, sia di misure volte ad evitare accessi da parte di soggetti pubblici che non siano necessari e proporzionati in una società democra-

tica). Le autorità di protezione dei dati sono tenute infatti ad esercitare i propri poteri di sospendere o vietare i trasferimenti nei casi in cui le salvaguardie addotte, di volta in volta, da ciascun titolare non siano considerate sufficienti. I poteri di controllo delle autorità saranno utilizzati ove possibile in modo coordinato, specie nel caso in cui istituzioni UE e Stati membri non individuino una soluzione politica che tenga conto della necessità di rispettare l'essenza del diritto fondamentale alla protezione dei dati anche in occasione dei trasferimenti di dati in Paesi terzi.

Alla luce della sentenza, la Commissione europea e gli Stati Uniti, già da tempo impegnati sul tema dei trasferimenti dei dati nell'ambito del processo di revisione del *Safe Harbour* avviato nel 2013 (cfr. Relazione 2013, p. 181), hanno proseguito le negoziazioni al fine di definire un nuovo quadro di riferimento per la protezione dei flussi transatlantici dei dati personali che tenga conto dei rilievi mossi dalla Corte di giustizia e superi tutti i dubbi in ordine all'adeguatezza del precedente sistema (cfr. anche Relazione 2014, p. 178): nel febbraio 2016 la Commissione ha così reso disponibile la documentazione relativa ad un nuovo sistema denominato "EU-US *Privacy Shield*" (comprendente una bozza di decisione di adeguatezza e le lettere di impegni degli organismi statunitensi competenti) che, ove considerato adeguato dalla Commissione medesima ai sensi dell'art. 25 della direttiva 95/46/CE, potrà consentire il libero trasferimento di dati personali verso le società statunitensi che vi aderiranno.

Soggetti pubblici e trasferimenti di dati personali

Sempre in tema di trasferimenti di dati verso Paesi terzi, il Gruppo ha lavorato sul tema dei trasferimenti di dati personali tra istituzioni e soggetti pubblici per finalità di cooperazione amministrativa. In materia, si ravvisa la necessità che i principi di protezione dei dati siano tenuti in considerazione nella predisposizione degli accordi per il trasferimento di dati tra soggetti pubblici UE e non-UE quando il Paese di destinazione non assicura una protezione adeguata, anche attraverso specifiche clausole che riguardino, in particolare, la liceità del trattamento, la proporzionalità e la qualità dei dati, il principio di finalità, la conservazione dei dati, le misure di sicurezza, i trasferimenti ulteriori di dati, la clausola di supervisione.

Bcr for controller* e *Bcr for processor

Con riguardo ai trasferimenti di dati verso Paesi terzi, continua l'attività di cooperazione del Garante nel quadro della procedura per l'adozione, a livello europeo, delle regole vincolanti d'impresa (Bcr) che possono essere utilizzate per il trasferimento dei dati effettuato tra società appartenenti ad un medesimo gruppo che operino in qualità di titolare del trattamento (*Bcr for controller*, Bcr-C) o in qualità di responsabili del trattamento (*Bcr for processor*, Bcr-P). Nel 2015 sono state avviate 13 procedure per Bcr-C e 3 per Bcr-P e sono state concluse, con il riconoscimento dell'adeguatezza delle disposizioni nelle stesse contenute, 10 Bcr-C e 2 Bcr-P (per le autorizzazioni nazionali v. cap. 17).

L'Autorità ha partecipato in qualità *co-reviewer* in 5 procedure fornendo specifiche indicazioni in ordine a modifiche da apportare nel testo delle Bcr proposte dalle società al fine di renderle conformi al quadro normativo europeo.

22.4. *La cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni*

Europol: l'attività dell'Autorità di controllo comune (ACC)

Come per il 2014, l'ACC Europol – che si è riunita quattro volte nel corso dell'anno – ha concentrato la propria attenzione sul processo legislativo relativo della proposta di regolamento che istituisce l'Agenzia dell'Unione europea per la cooperazione e la formazione delle autorità di contrasto (Europol) e abroga le decisioni nn. 2009/371/GAI e 2005/681/GAI del Consiglio (presentata nel 2013 dalla

Commissione europea, doc. web n. 2983062) e sulla necessità di garantire, attraverso la propria attività ispettiva ed i propri sottogruppi, che i trattamenti di dati personali siano effettuati da Europol nel rispetto della disciplina di protezione dei dati.

Con riferimento al nuovo quadro normativo, la cui definizione risulta imminente alla luce dell'accordo che sembra essere stato raggiunto alla fine dell'anno dalle tre istituzioni europee nell'ambito del trilogo, l'ACC (nelle persone della presidente Vanna Palumbo e vicepresidente Wilbert Tomesen) ha incontrato, il 22 giugno, il relatore della proposta di regolamento al Parlamento europeo per discutere alcuni aspetti sostanziali del nuovo quadro giuridico e, in particolare, il tema della supervisione. In proposito è stata ribadita la necessità, già evidenziata nei pareri espressi dall'ACC sulla proposta di regolamento (doc. web nn. 2983184, 2983132 e 3815594), di mantenere un ruolo effettivo alla cooperazione tra le Autorità nazionali di protezione dati, attesa la complessità del sistema e la rilevanza dell'attività di Europol per le attività giudiziarie e di polizia nazionali. Tale cooperazione dovrebbe, in effetti, essere garantita dal nuovo regolamento che attribuisce la supervisione all'EDPS coadiuvato da un Gruppo di coordinamento composto da rappresentanti delle DPA nazionali.

Alla luce dell'entrata in vigore del nuovo testo – attesa per la primavera del 2017 – l'ACC ha iniziato a riflettere sul futuro della supervisione su Europol, costituendo un gruppo di lavoro con il compito di approfondire il tenore dei cambiamenti ed in particolare di identificare i compiti che il Gruppo di coordinamento dovrà svolgere e la continuità/discontinuità con le attività svolte finora nonché gli aspetti logistici, organizzativi (segretariato, regolamento interno) e finanziari.

Per quanto riguarda l'attività ispettiva, nel marzo 2015, come di consueto, si è svolta l'ispezione annuale di Europol, effettuata in modo particolarmente approfondito per verificare il rispetto di tutte le prescrizioni impartite negli anni, lo stato della loro attuazione ed il livello di criticità di quelle non adempiute.

A maggio 2015, l'ACC ha poi svolto un'ispezione dedicata alle attività poste in essere da Europol in relazione all'Accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP - *Terrorist Finance Tracking Program*). Nel relativo rapporto (adottato a settembre 2015, doc. web n. 4810393) – che, nel complesso, valuta l'attività svolta dal dicembre 2012 al maggio 2015 come conforme alla disciplina di riferimento – l'Aurorità ha ribadito che persiste una tensione rra l'idea di limitare la quantità di dati trasmessi ai sensi dell'art. 4 dell'Accordo con la natura dell'Accordo medesimo sulla base del quale, comunque, persiste un trasferimento massivo e regolare di informazioni finanziarie dall'Unione europea agli USA.

All'esito dell'approfondimento relativo al tema del traffico di esseri umani, avviato nel 2014 sulla scorta dell'esperienza maturata da Europol e Eurojust (che tratrano e analizzano anche i dati personali relativi alle vittime di tale rraffico trasmessi dalle autorità di contrasto degli Stati membri dell'UE e da parti terze), l'Autorità ha poi adottato un Rapporro sulle vittime della tratta di esseri umani (doc. web n. 4814921). Il documento, predisposto anche al fine di migliorare la qualità dei dati contenuti negli archivi Europol e sviluppare una maggiore attenzione all'identificazione precoce delle vittime, constata che, a livello sia nazionale che internazionale, le attività di trattamento dei dati condotte da tutte le autorità competenti (polizia, pubblici ministeri e giudici istruttori) dovrebbero essere caratterizzate da un'attenzione e un'armonizzazione maggiori. Il rispetto dei princìpi di necessità, proporzionalità, finalità e qualità dei dati relativi alle vittime della tratta risulta infatti essenziale nel quadro del più ampio fine della prorezione

22

di questi soggetti. La relazione è stata anche sostenuta dall'Autorità di controllo comune di Eurojust.

Nel 2015, è continuata anche l'attività dei sottogruppi dell'ACC. Si è infatti riunito il Comitato ricorsi e, più volte, il *New Project Group*. Quest'ultimo, in particolare, ha proseguito la propria valutazione sul progetto per la creazione di una lista europea degli individui più ricercati (*EU Most Wanted List*) in relazione al quale l'ACC ha espresso forti perplessità per la mancanza, nel quadro giuridico esistente, di una apposita base giuridica che consenra ad Europol di svolgere questo trattamento come titolare del trattamento.

Il Sistema Informativo Schengen: l'attività del Gruppo di coordinamento della supervisione SIS II

Il Gruppo di coordinamento della supervisione SIS II ha avviato, con una visita realizzata a settembre 2015, insieme con i gruppi di coordinamento della supetvisione VIS e Eurodac (v. *infra*) un'attività di narura "conoscitiva" sui trattamenti posti in essere dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (EU-LISA) presso il *data center* di Strasburgo all'interno del quale sono ospitate le banche dati SIS, VIS e Eurodac. Lo scopo della visita, coordinata dai *Data Protection Officer e Data Security Officer* di EU-LISA, è stato quello di acquisire prime informazioni sull'architettura dei sistemi e sulle misure di sicurezza adottate.

Il sottogruppo sta inoltte lavorando su modelli comuni – uno per l'*audit* del SIS II e l'altro per le ispezioni – che potranno essere impiegati per attività ispettive in ambito nazionale da patte delle DPA, in modo da garantire il massimo grado di armonizzazione con le azioni svolte a livello centralizzato nel nuovo quadro di supervisione a livello EU.

Il Gruppo ha continuato ad occuparsi dei criteri per l'introduzione nel sistema delle segnalazioni concernenti i veicoli rubati con l'idea di elaborare una posizione comune su come interpretare le disposizioni relative alle azioni da intraprendere nel caso in cui un veicolo segnalato come tubato nel SIS venga localizzato in altro Paese e se debba prevalere la buone fede dell'acquirente laddove non sia richiesta la restituzione/sequestro del mezzo con conseguente cancellazione della segnalazione.

Gruppo di supervisione Eurodac

In relazione all'entrata in vigore (il 20 luglio 2015) della nuova base giuridica derivante dall'adozione, il 26 giugno 2013, della proposta di rifusione (cd. *recast*) del regolamento Eurodac (regolamento (UE) n. 603/2013: cfr. Relazione 2013, p. 186, doc. web n. 2983052), il Gruppo di supervisione del sistema Eurodac (che ha eletto come presidente Elisabeth Wallis e nuovo vice Andres Ojaver) sta lavorando su un rapporto che fornisca un quadro delle modalità con cui il sistema è utilizzato nei divetsi Stati membri.

Per valutare l'impatto dell'entrata in vigore del nuovo quadro giutidico e al fine di acquisire prime informazioni sull'architettura dei sistemi e sulle misure di sicurezza adottate, il 22 settembre, il Gruppo ha poi effettuato una visita al *data center* dell'Agenzia EU-LISA, all'interno del quale sono ospitate le banche dati SIS, VIS e Eurodac. Si è trattato di una visita ricognitiva, coordinata *dai Data Protection Officer* e *Data Security Officer* dell'Agenzia stessa, che ha consentito di avere una chiara visione delle misure di sicurezza fisiche e logiche adotrate. In tale occasione, il Gruppo ha insistito sulla necessità che EU-LISA ponga adeguata attenzione alla materia della protezione dei dati nell'opera di formazione che svolge nei confronti degli utilizzatori del sistema (tra cui, dalla data di entrata in vigore del nuovo regolamento, anche le autorità di *law enforcement*).

Il Sistema Informativo Visti (VIS): Gruppo di coordinamento della supervisione

Il Gruppo di coordinamento della supervisione VIS (che ha eletto come presidente Vanna Palumbo del Garante e come vicepresidente il rappresentanre dell'autorità spagnola, Manuel Garcia) si è riunito due volte ed ha proseguito l'attività avviata nel 2015 volta a verificare il funzionamento del sistema nei diversi Paesi membri. A tal fine, sono state raccolte le risposte ai tre questionari definiti,

definiti nel 2014, volti a chiarire gli assetti nazionali del sistema in relazione all'elenco delle autorità che lo utilizzano; all'accesso al sistema per finalità di *law enforcement* e alle modalità per l'esercizio dei diritti degli interessati. Il Gruppo sta inoltre lavorando sulle forme di esternalizzazione delle procedure di raccolta dei dati nell'ambito degli *iter* amministrativi relativi al rilascio dei visti. Oggetto di valutazione saranno, in particolare, i contratti utilizzati dai Paesi membri per esternalizzare tali attività e la loro conformità rispetto agli *standard* di protezione dei dati.

Alle riunioni, come di consueto, i membri del gruppo si sono incontrati con i rappresentanti della Commissione e l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (EU-LISA) per discutere dello stato di avanzamento del VIS *roll-out*, i previsti ulteriori *roll-out*, i recenti sviluppi relativi alla qualità dei dati nel sistema e il ruolo dei subappaltatori.

Il Gruppo ha poi adottato il programma di lavoro per il periodo del 2015 al 2018 che individua, tra i temi da affrontare, il trasferimento di dati a Paesi terzi o organizzazioni internazionali, la cancellazione anticipata dei dati, la formazione del personale in materia di sicurezza e norme sulla protezione dei dati e l'auto-monitoraggio delle autorità che hanno accesso al VIS.

Il Gruppo ha adottato anche la relazione delle attività svolte nel biennio 2012-2014 che include un capitolo nazionale per ciascuno dei trenta Paesi che utilizzano il VIS, vale a dire tutti gli Stati Schengen, tutti e quattro gli stati membri dell'area europea di libero scambio – Islanda, Liechtenstein, Norvegia e Svizzera e Bulgaria, Croazia, Cipro e Romania, che non sono ancora parte dello spazio Schengen, ma comunque hanno una politica dei visti sulla base di Schengen.

La visita svolta il 22 settembre presso il *data center* di EU-LISA, a Strasburgo, all'interno del quale sono ospitate le banche dati SIS, VIS e Eurodac, ha infine consentito al Gruppo di avere un primo quadro sul funzionamento del sistema e sulle misure di sicurezza adottate.

Il Sistema informativo doganale (SID): ACC Dogane e Gruppo di coordinamento della supervisione SID

L'ACC Dogane e il Gruppo di coordinamento della supervisione del Sistema informativo doganale (SID) – che come di consueto si sono riunite *back to back* due volte l'anno – hanno continuato la propria attività di supervisione del sistema informativo che raccoglie le informazioni volte a prevenire, ricercare e perseguire le operazioni contrarie alle regolamentazioni doganale o agricola (sulla base, rispettivamente, della decisione 2009/917/GAI e della decisione quadro 2008/977/GAI per i trattamenti effettuati per facilitare la prevenzione, la ricerca e il perseguimento di gravi infrazioni alle leggi nazionali e del regolamento (EC) No 515/1997, artt. 23 e ss. relativo alle violazioni di natura amministrativa.

In particolare, l'ACC Dogane ha curato, attraverso le DPA che in essa sono rappresentate, la diffusione del *leaflet* (tradotto nelle diverse lingue dell'Unione) dal titolo "*Guide to your responsabilities under Article 13 of the CIS Decision and art. 8(2) della Data protection framework decision*" (in italiano doc. web n. 4349259) che ha lo scopo di fornire alcune indicazioni in ordine alle modalità che le Autorità competenti per il sistema sono tenute a seguire ove risulti necessario correggere, rettificare o cancellare eventuali informazioni inesatte o inserite nel sistema in violazione di legge. L'Autorità ha poi iniziato a valutare le risposte pervenute dall'Olaf e dalle autorità nazionali al questionario inviato come *follow up* delle raccomandazioni espresse dopo l'ispezione del sistema svoltasi nel 2011.

Nel corso dell'anno il Gruppo di coordinamento della supervisione del SID (che ha eletto come nuovo presidente Piotr Drobek, delegato della DPA polacca e ha esteso il proprio programma di lavoro 2014-2015 fino alla fine del 2016) ha lavorato su un possibile modello comune per le attività ispettive che le DPA, ove neces-

sario, possono porre in essere con riferimento al sistema SID e ha ultimato i lavori per la predisposizione della guida all'esercizio dei diritti di accesso allo stesso (doc. web n. 4810368). La guida fornisce indicazioni precise su come gli interessati possono esercitare i propri diritti nei diversi Stati membri, fornendo anche indicazioni sulle autorità da contattare.

22

22.5. *La partecipazione ad altri comitati e gruppi di lavoro internazionali*

Consiglio d'Europa – T-PD

Nell'ambito del Consiglio d'Europa il Garante ha proseguito la partecipazione all'attività del T-PD, Comitato consultivo della Convenzione 108/1981, anche nella sua composizione ristretta (T-PD *Bureau*).

Il T-PD ha continuato a seguire il processo di modernizzazione della Convenzione 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, volto ad adeguarne i princìpi al mutato scenario tecnologico e a garantire la tenuta di un alto livello di protezione dei diritti delle persone (vedi Relazione 2014, p. 183). Tale processo pur avendo portato, già nel dicembre 2014, all'adozione – da parte del comitato intergovernativo *ad hoc* CAHDATA – della Convenzione modernizzata (fondata sul testo adottato dal T-PD nella plenaria del 18 dicembre 2012, vedi Relazione 2012, p. 298), non si è ancora concluso. Il protocollo emendativo della Convenzione 108 predisposto dal segretariato del Consiglio d'Europa sulla base del documento adottato dal CAHDATA non è stato infatti ancora adottato dal Comitato dei ministri, in ragione delle persistenti riserve, tra cui quelle della Commissione europea su alcuni articoli corrispondenti a nodi non ancora sciolti dal nuovo regolamento UE.

Il T-PD ha inoltre continuato a lavorare alla predisposizione del *memorandum* esplicativo della Convenzione 108 in modo da allinearlo alle diverse novità inserite nella Convenzione modernizzata.

Nell'ambito delle attività del T-PD è inoltre proseguito il lavoro di attualizzazione dei princìpi di protezione dei dati in ambito sanitario in particolare con riferimento all'impiego di nuove tecnologie nel settore medico (fascicoli sanitari elettronici, *app* mediche, RFID, tecniche di profilazione, ecc.) che ha portato all'elaborazione di un progetto di revisione della raccomandazione (97)5 sul trattamento dei dati sanitari.

Il Comitato ha inoltre approfondito il tema *big data*, con la predisposizione di una bozza di linee guida volte ad esaminare le diverse problematiche emerse in tale settore e a declinare i princìpi di protezione dei dati.

Una prima bozza di parere sul tema delle informazioni relative ai passeggeri aerei è stata inoltre discussa dal Comitato in vista di una sua possibile adozione nel corso del 2016.

Altri temi che sono stati all'attenzione del T-PD riguardano le implicazioni sulla protezione dei dati provenienti dagli scambi automatizzati di dati tra Stati in relazione alla lotta all'evasione fiscale, al riciclaggio, al finanziamento del terrorismo e alla corruzione, ai profili di *privacy* nell'ambito delle politiche di ICANN, e al trattamento dei dati in ambito di polizia, che sarà oggetto di ulteriori approfondimenti in vista dell'elaborazione di una guida pratica per gli operatori del settore.

Il Comitato dei ministri del Consiglio d'Europa, nella riunione del 1° aprile ha adottato la raccomandazione (2015)5 sulla protezione dei dato in ambito lavorativo che ha così completato il lavoro del T-PD che aveva approvato il testo nella plenaria di giugno del 2014 (v. Relazione 2014, p. 183). La nuova raccomanda-

22

OCSE

zione sostituisce la raccomandazione (89)2, ampliandone i princìpi e declinandoli alla luce delle nuove tecnologie in uso nel mondo del lavoro, in particolare con riferimento all'impiego di *e-mail* e internet da parte del dipendente, al controllo a distanza del lavoratore, al trattamento di dati biometrici e genetici (doc. web n. 4814881).

L'Autorità ha continuato a partecipare ai lavori del SPDE (*Working Party on Security and Privacy in Digital Economy Working Party on Information Security and Privacy*) dell'OCSE. Nel 2015 il Garante, già membro del Gruppo e componente del *Bureau* dello stesso, è stato riconfermato nel *Bureau* del SPDE anche per il 2016.

Gran parte del lavoro del Gruppo è stato dedicato alla preparazione della Ministeriale 2016 che l'OCSE terrà a Cancun (Messico) il 21-23 giugno 2016. Il tema della Ministeriale è la "*Digital Economy:* Innovazione, Crescita e sociale Prosperità" e se ne discuterà in quattro sezioni, con due sezioni plenarie di apertura e chiusura. La responsabilità principale per lo SPDE è l'organizzazione del *panel* dal titolo "*Public/Private Cooperation in Managing Digital Security and Privacy Risk for Economic and Social Prosperity*". Nel corso dell'anno il Gruppo si è perranto concentrato sul tema centrale di tale sessione, ossia la protezione dati in ambito digitale con riferimento ad "un approccio basato sul rischio" (cd. *risk based approach*, come previsto anche dal regolamento europeo sulla protezione dei dati la cui pubblicazione è prevista sulla GUUE del 4 maggio 2016; v. par. 22.1). Lo SPDE ha inoltre contribuito alla preparazione di altri *Panel* della Ministeriale, in particolare delle sessioni dedicate rispettivamente ai vantaggi economici e sociali di un *Open Internet* e alla *Internet delle cose* (*IoT*).

Gli esiti della Ministeriale confluiranno in una dichiarazione ministeriale che potrebbe approvare il lavoro che l'OCSE effettua per sostenere lo sviluppo dell'economia digitale e fornire indicazioni per il lavoro futuro, anche da parte dello SPDE. Il Gruppo si è impegnato nella redazione della bozza di Dichiarazione che nella sua ultima versione di dicembre 2015 appare semplificata rispetto alla precedenti versioni. La bozza, in corso di aggiornamento, riconosce il valore e, allo stesso tempo, la pervasività delle tecnologie digitali e auspica un approccio il più possibile fondato sulla cooperazione e sull'inclusione dei diversi attori in gioco, al fine di cogliere appieno i benefici dell'economia digitale e facilitare l'adozione di standard tecnici comuni, nel rispetto della protezione dei dati personali.

Oltre al tema della Ministeriale, lo SPDE nel corso del 2015 ha anche ultimato il lavoro di revisione della raccomandazione sulla Sicurezza del 2002 (*Recommendation Concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security:* "OECD *Security Guidelines*"). Tale lavoro ha portato, nel mese di settembre, all'adozione della nuova raccomandazione sulla sicurezza digitale (*Recommendation on Digital Security Risk Management for Economic and Social Prosperity*, doc. web n. 4295203). Nel documento l'OCSE sostiene che il rischio per la sicurezza digitale dovrebbe essere considerato un problema di ordine economico e non solo tecnologico, e dovrebbe essere integrato nei processi decisionali di ogni organizzazione. Il lavoro del Gruppo ha fatto emergere come un ambiente digitale globale, interconnesso, aperto e dinamico generi notevoli opportunità economiche, ancora più promettenti se si pensa alla crescente diffusione dell'internet delle cose e dei *big data*. Tuttavia, Paesi e aziende sono esposti a minacce sempre più sofisticate e crescenti che possono mettere in pericolo la sicurezza delle informazioni e compromettere la prosperità economica e sociale. La raccomandazione dell'OCSE sulla *digital security* chiede quindi a governi e vertici aziendali di assumersi la specifica responsabilità della gestione del rischio della sicurezza digitale integrandola nella pianificazione generale. L'OCSE indica otto princìpi-guida per la gestione del rischio riferito alla sicurezza

digitale, anche con riguardo alla responsabilità dei diversi soggetti, alla cooperazione tra le parti interessate e al ruolo dell'innovazione. In particolare, si raccomanda l'adozione di piani nazionali per individuare le misure utili a prevenire, affrontare e sanare le conseguenze di incidenti di sicurezza digitale. La raccomandazione rappresenta una solida base per attuare anche molti dei princìpi contenuti nelle *Privacy Guidelines* dell'OCSE (v. Relazione 2014, p. 185) e i due strumenti si integrano perfettamente. Il Gruppo di lavoro si è quindi adoperato negli ultimi mesi dell'anno nella promozione della Raccomandazione attraverso la massima divulgazione del testo.

Tra gli altri temi, si segnala infine il lavoro dell'OCSE sulla protezione e sicurezza dei dati in ambito sanitario portato avanti dallo SPDE e dal neoistituito *Oecd Advisory Expert Group*, il Gruppo consultivo di esperti per guidare lo sviluppo della proposta di Raccomandazione sull'uso dei dati sanitari (*Draft Council Recommendation on privacy protective approaches for the use of personal health data*). Nel mese di novembre si è tenuto il primo incontro della *task force*. All'incontro hanno partecipato trenta esperti (tra cui due esperti del Garante) di almeno undici Paesi e sono emerse significative differenze nei sistemi di cura della salute e nell'uso delle terminologie del settore. Oggetto dell'incontro è la stata la bozza della citata raccomandazione. Dal testo (in corso di aggiornamento) emerge come la raccomandazione miri alla ricerca di un sistema sanitario migliore e più efficiente nei Paesi OCSE, fornendo Linee guida ai decisori dei diversi Paesi nello sviluppo di *framework* di *governance* o di riforme in materia di *governance* dei dati sanitari laddove trattati per la salute pubblica, scopi scientifici e di ricerca, per statistiche del sistema sanitario e per migliorare la gestione e la fornitura di servizi di assistenza sanitaria. Il documento si basa sui princìpi enunciati nelle *Privacy Guidelines* dell'OCSE, in particolare, su specifiche previsioni in esse contenute in relazione al trattamento dei dati sanitari (dati sensibili).

Progetto *Big Data Ethical Assessment Process*

Nel 2015 il Garante ha altresì partecipato al *workshop Big Data Ethical Assessment Process*, progetto *multi-stakeholder* organizzato dall'*Accountability Foundation*, volto a indirizzare i diversi titolari del trattamento (soggetti privati) che gestiscono *big data* verso un orientamento etico e responsabile.

Nel corso dell'anno si sono tenuti due incontri, rispettivamente a Madrid il 29 aprile presso l'Autorità spagnola e a Roma presso il Garante il 14 luglio. Si è discusso dei possibili strumenti da approntare al fine di assicurare un quadro di princìpi etici nella gestione dei *big data* come sfida globale per i diritti umani, inclusi il diritto alla protezione dei dati e *privacy*.

Mentre la prima riunione si è concenttata sulla possibilità di realizzare un codice etico vincolante per *big data*, prevedendo specifiche competenze in capo alle Autorità di regolamentazione per rendere applicabile tale codice di condotta anche a livello nazionale, nel secondo incontro si è proposto di focalizzare l'attenzione su una lista di raccomandazioni relative alla dimensione etica del trattamento dei dati nel contesto *big data*. In tale ambito, sono state affrontate diverse tematiche, tra cui i poteri di *enforcement* delle autorità di protezione dati e la loro effettività, l'anonimizzazione e la minimizzazione dei dati, le garanzie per assicurare un'effettiva cancellazione dei dati, la dimensione pubblica del *big data* (per la ricerca) e la promozione di una *governance* responsabile da parte delle aziende anche attraverso *standard* internazionali.

IWGDPT

L'Autorità ha proseguito la sua partecipazione all'*International Working Group on Data Protection in Telecommunication* (IWGDPT, cd. Gruppo di Berlino) che nel corso del 2015 si è riunito a Seul il 27-28 aprile e a Berlino il 14 e 15 ottobre.

Nella prima riunione il Gruppo ha lavorato sul tema della *accountability* delle imprese in caso di accesso da parte di autorità pubbliche ai dati personali in loro possesso. Il Gruppo si è soffermato in particolare sul cd. *transparency reporting*, consistente nella pubblicazione periodica, da parte di alcune società di statistiche e

caratteristiche dei dati personali trasmessi, per finalità diverse da quelle commerciali, a terze parti, in particolare alle autorità di polizia. Con l'adozione di uno specifico documento di lavoro su tale argomento, il Gruppo ha richiamato l'attenzione sui princìpi di protezione dei dati cui tale attività deve ispirarsi ed ha fornito raccomandazioni per la loro attuazione ai diversi attori coinvolti (imprese, legislatori, autorità pubbliche che richiedono l'accesso, autorità di protezione dei dati, organizzazioni internazionali e società civile) (doc. web n. 4814944).

È stato inoltre adottato un documento di lavoro sui cd. *wearable computing devices*, dispositivi digitali indossabili che, dotati di specifici sensori, permettono la raccolta in tempo reale di dati personali (doc. web n. 4814934). Anche questo documento fornisce una serie di raccomandazioni volte a garantire il rispetto dei princìpi *privacy* nel settore, affinché sia assicurato il controllo da parte dell'interessato dei dati che lo riguardano, la trasparenza dei trattamenti effettuati (dei quali spesso – per le caratteristiche dei dispositivi stessi – l'interessato è poco consapevole), l'agevole esercizio dei diritti, e la portabilità dei dati. Particolare attenzione è dedicata al trattamento di dati sensibili, che deve essere subordinato alla prestazione del consenso esplicito dell'interessato, e all'impiego di tali dispositivi in ambito lavorativo perché sia adeguatamente tutelata la libertà di scelta del lavoratore.

Con un documento di lavoro adottato nella riunione di Berlino, il Gruppo è tornato ad occuparsi del tema della localizzazione derivante dall'impiego di dispositivi mobili (doc. web n. 4814975). Specifiche raccomandazioni mirano ad assicurare che tali trattamenti avvengano nella piena consapevolezza degli interessati, siano proporzionati alla legittima finalità perseguita, i dati siano anonimizzati non appena raggiunto lo scopo, la combinazione dei dati con altre informazioni e la comunicazione a terzi avvengano con il consenso dell'interessato e siano garantiti agli interessati idonei strumenti per esercitare il controllo sui propri dati.

Nella stessa riunione il Gruppo ha anche trattato il tema delle tecniche di *intelligent video analytics* (ad es., videosorveglianza intelligente), che consentono l'osservazione di comportamenti e caratteristiche degli individui per diverse finalità, tra cui la personalizzazione di comunicazioni commerciali e di prezzi di prodotti o servizi, la rilevazione di comportamenti anomali a fini di sicurezza e l'ottimizzazione di servizi (doc. web n. 4814956). Tali tecniche, pur perseguendo finalità legittime, devono essere congegnate e utilizzate tenendo conto del loro impatto su *privacy* e protezione dei dati personali, anche per evitare un effetto frenante sull'esercizio di alcuni diritti e libertà fondamentali, quali la libertà di espressione o di assemblea.

Tra gli altri temi trattati dal Gruppo nel corso dell'anno, anche in vista di futuri approfondimenti, si segnalano infine: il ricorso a strumenti di *e-learning* da parte dei sistemi scolastici nazionali, mediante specifiche applicazioni per terminali mobili (*tablet*), che utilizzano tecniche di identificazione dei terminali (e indirettamente degli utenti) basate sull'uso di *cookies*; nuove forme di autenticazione sul web, in particolare sulla base di tecniche di riconoscimento biometrico, non più dunque basate sull'uso di *password* e di facile impiego per gli utenti con l'obiettivo di incrementare la sicurezza; il tema del cd. *delisting* dai risultati offerti da un motore di ricerca; gli aspetti di *privacy* e sicurezza connessi all'uso di servizi VoIP; gli sviluppi in materia di standardizzazione con particolare riferimento alle modalità *user friendly* per l'acquisizione del consenso e sulla de-identificazione; le problematiche *privacy* nei *social networks*.

Cooperazione internazionale IECWG, GPEN, PHAEDRA *project*

Nel 2015 è proseguita l'attività dei Gruppi di lavoro dedicati al coordinamento delle attività internazionali di *enforcement*, come richiesto dalla 36ª Conferenza internazionale delle autorità di protezione dati (v. Relazione 2014, p. 187) e dal lavoro del Gruppo di coordinamento delle attività internazionali di *enforcement* (IECWG).

In tale contesto, si è intensificata l'attività del *Global Privacy Enforcement Network*-GPEN, la prima rete internazionale di cooperazione transfrontaliera in tema di *enforcement* lanciata nel 2010 (v. par. 22.2). Su *input* del GPEN, il Garante (membro del Gruppo) ha svolto il 12 maggio lo *Sweep* 2015 dedicato alla protezione in rete dei minori tra gli 8 e i 13 anni. Sono stati analizzati decine di siti internet tra i più visitati da bambini e alcune delle più diffuse *app* per minori (fino a 13 anni) scaricabili su *smartphone* e *tablet*. I risultati dell'indagine svolta hanno mostrato che le *app* e i siti internet più utilizzati dai bambini italiani non tutelano adeguatamente la *privacy* dei piccoli utenti. Nello specifico, gli esperti del Garante hanno selezionato 22 *app* e 13 siti internet (appartenenti al settore *educational*, al mondo dei giochi, a servizi *online* offerti da canali televisivi per l'infanzia, ai *social network*) tra i più popolari tra i bambini, o appositamente sviluppati per loro, e ne hanno analizzato le caratteristiche. Tra i 35 casi analizzati dagli *sweepers* del Garante ben 21 hanno evidenziato gravi profili di rischio e 8 di questi richiederanno specifiche attività ispettive. È emerso un panorama critico, in linea con le problematiche riscontrate anche dalle altre Autorità internazionali. I risultati evidenziano una grave disattenzione nei confronti dei più piccoli, poca trasparenza in merito alla raccolta, all'utilizzo dei dati personali e alle autorizzazioni richieste per scaricare le *app* su *smartphone* e *tablet*, presenza di pubblicità e rischi che i bambini vengano reindirizzati verso siti non controllati (doc. web n. 4234002).

XXVII *Case Handling workshop*

Si è tenuto a Tirana, il 28 e 29 settembre, il 27° *Case Handling workshop*, l'incontro annuale nel corso del quale le autorità si confrontano sui casi pratici affrontati a livello nazionale. Diversi i temi approfonditi nel *workshop* di quest'anno, in particolare l'utilizzo dei droni e altre forme "intelligenti" di videosorveglianza, il *credit reporting*, il trattamento dei dati del sistema bancario e la profilazione. L'incontro è stato anche occasione di scambio con riferimento alle modalità di gestione di ricorsi e reclami, e alle attività di cooperazione tra diverse autorità, come quella intercorsa tra il Garante e l'autorità albanese in mareria di trattamento dei dati da parte dei *call center* (v. *infra*).

Incontri con le delegazioni estere e organizzazioni internazionali

L'Autorità ha continuato a partecipare a programmi di partenariato europeo negli ambiti di competenza, offrendo la propria esperienza per facilitare l'avvicinamento delle normative dei Paesi coinvolti al quadro comunitario in materia di protezione dei dati. Nel mese di febbraio si è tenuta la visita, presso il Garante, di una delegazione dell'Autorità per la protezione dei dati albanese. Durante la visita – che ha permesso l'approfondimento di diversi temi tra cui la possibilità di ispezioni congiunte tra il Garante italiano e quello albanese con riferimento ai *call center* – è stato firmato l'Accordo di cooperazione tra le due autorità.

Nell'ambito del Progetto TAIEX della Commissione europea, si è tenuto il 31 marzo, a Podgorica, un *workshop* in tema di protezione dei dati nel contesto della videosorveglianza, cui il Garante ha partecipato, che aveva lo scopo di richiamare l'attenzione delle autorità pubbliche montenegrine sul tema.

23 L'attività di comunicazione, informazione e di rapporto con il pubblico

23.1. *La comunicazione del Garante: profili generali*

Il Garante ha da sempre considerato l'attività di informazione e comunicazione istituzionale fondamentale per la diffusione di una cultura della protezione dei dati nel nostro Paese. In quest'ottica già da qualche anno l'Autorità ha rafforzato la sua azione anche nei canali *social*, puntando anche alla produzione multimediale destinata al web.

Uno dei grandi temi che nel corso del 2015 l'Autorità si è trovata nuovamente ad affrontare è stato quello del rapporto tra sicurezza *e privacy*, con particolare riferimento alle problematiche legate alle intercettazioni, alla conservazione dei dati di traffico sia telefonico che telematico, al tracciamento dei passeggeri dei voli, alla sorveglianza di massa, anche alla luce degli attacchi terroristici che si sono succeduti in ogni parte del mondo, giungendo fin nel cuore dell'Europa. Proprio il bisogno di sicurezza ed il ricorso all'uso di avanzate tecnologie per il controllo di massa rischiano di compromettere i modelli di protezione dei dati personali e le libertà fondamentali delle società democratiche. Su tali delicate questioni il Garante è più volte intervenuto sottolineando la necessità di assicurare un bilanciamento tra i menzionati diritti tra loro in tensione.

Riguardo, in particolare, alla lotta al terrorismo l'Autorità ha affermato che occorre mettere in campo una raccolta selettiva e non generalizzata delle informazioni in quanto l'enorme accumulazione di informazioni fin qui realizzata in grandi banche dati pubbliche e private non sufficientemente protette rischiano di allargare a dismisura la superficie di attacco del terrorismo. La minaccia più grave oggi è rappresentata dal *cybercrime* e diventa dunque primaria la necessità che le grandi infrastrutture strategiche del nostro Paese vengano protette in maniera efficace è indispensabile.

In relazione allo sviluppo di una forte consapevolezza del valore dei dati personali e dell'importanza di una loro tutela soprattutto nel mondo *online*, il Garante ha concentrato il suo impegno su alcune grandi problematiche: i *social network* e i pericoli derivanti dalla diffamazione in rete: *l'hate speech* e il *cyberbullismo*; il diritto all'oblio, il *cybercrime* ed il furto d'identità; l'interner delle cose (Iot). Proprio quest'ultimo tema è stato al centro dei lavori del convegno "Il pianeta connesso. La nuova dimensione della *privacy*", organizzato dal Garante in occasione della celebrazione della Giornata europea della protezione dei dati personali.

Altre questioni di particolare rilievo sociale trattate nel periodo di riferimento sono state la trasparenza della p.a. *online* e le garanzie da assicurare ai cittadini, il fisco e la tutela delle riservatezza dei contribuenti, l'uso delle nuove tecnologie sul posto di lavoro, il *telemarketing* selvaggio, i diritti dei consumatori, la scuola, i partiti e i movimenti politici, la dichiarazione di volontà per la donazione degli organi sui documenti di identità. Anche il settore della sanità ha rappresentato un altro ambito sul quale si è concentrato l'impegno dell'Autorità, a partire dal fascicolo e dal *dossier* sanitario elettronico sino alle tutele da riservare agli assistiti riguardo alla sicurezza dei loro dati personali.

È stata condotta dall'Autorità italiana, in collaborazione con altre ventisette autorità internazionali facenti parte del *Global Privacy Enforcement Network* (GPEN) una speciale indagine sulla *privacy* dei bambini e, in occasione del "*Privacy Sweep* 2015" dedicato alla protezione in rete dei bambini tra gli 8 e i 13 anni, ne sono stati resi noti gli esiti principali. I risultati dell'indagine hanno evidenziato che le *app* e i siti internet più utilizzati dai bambini italiani non tutelano a dovere la *privacy* dei piccoli utenti (in merito v. *amplius* par. 22.5).

Riguardo al preoccupante fenomeno del *cyberbullismo* e sulle azioni da mettere in campo per contrastarlo, il Garante ha dato il proprio contributo al Miur per l'elaborazione delle "Linee di orientamento per azioni di prevenzione e contrasto al *cyberbullismo*" presentate dal Ministro nel mese di aprile e trasmesse a tutte le scuole italiane.

L'Autorità ha inoltre fornito indicazioni per l'elaborazione di un sito informativo "Vivere in un mondo connesso" (www.mondoconnesso.info), realizzato da Facebook e lanciato anche in Germania, Austria e Francia, dedicato alla tutela dei dati personali su internet e nella vita quotidiana. Il sito, corredato anche di uno strumento di autovalutazione delle competenze in materia di *privacy online* sviluppato da Unione nazionale consumatori, consente di raggiungere in maniera diretta gli utenti dei *social network* affinché prestino maggiore attenzione alla tutela della *privacy* in rete.

I *media* hanno mantenuto una costante attenzione alle tematiche riguardanti la protezione dei dati personali e all'attività del Garante. Nel 2015 il Servizio relazioni esterne e *media* ha selezionato circa 57.200 articoli di interesse per l'Autorità. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali, delle testate *online* e *blog* che hanno trattato i temi legati alla *privacy* sono stare 14.685, delle quali 4.293 dedicate esclusivamente all'attività del Garante. Le prime pagine sono state oltre 980, di cui 212 riguardanti la sola Autorità. Le interviste, gli interventi e le dichiarazioni del presidente e dei componenti pubblicate sulla carta stampata sono state complessivamente 251, 343 quelle *online* e 34 quelle andate in onda su tv e radio nazionali e locali. Le citazioni relative al tema della *privacy* e all'attività del Garante in programmi televisivi e radiofonici nazionali sono state oltre 200.

23.2. *I prodotti informativi*

Nel 2015 sono stati diffusi 34 comunicati stampa e 13 *newsletter*, pubblicazione periodica giunta al suo XVII anno di diffusione (per un totale di 410 numeri e di 1.411 notizie), che consente un'approfondita divulgazione dei più importanti provvedimenti adottati dall'Autorità, della sua attività in ambito europeo ed internazionale e delle molteplici iniziative promosse. Le notizie pubblicate vengono redatte a cura del Servizio relazioni esterne e *media*, composte graficamente e completate con l'aggiunta di immagini per la versione web. La *newsletter* – che conta nella lista di distribuzione circa 8.000 destinatari – viene inviata via *e-mail* a redazioni, professionisti, operatori delle pp.aa., imprese e singoli cittadini che ne fanno richiesta. Sul sito del Garante è attiva l'opzione "Iscriviti alla *newsletter*" (a disposizione di tutti i visitatori, allo scopo di favorire una più ampia utilizzazione di questo importante strumento di informazione). È poi possibile consultare l'archivio tematico completo della *newsletter* che raccoglie tutti gli articoli finora pubblicati (cfr. sez. IV, tab. 2).

23.3. *I prodotti editoriali e multimediali*

Nuovi prodotti editoriali e multimediali si sono aggiunti alla già ricca collezione dell'Autorità.

Nell'ambito della Collana editoriale del Garante, "Contributi", è stato pubblicato il volume "Il pianeta connesso. La nuova dimensione della *privacy*" che raccoglie i contributi degli studiosi e degli esperti intervenuti al convegno organizzato dall'Autorità in occasione della celebrazione della Giornata europea della protezione dei dati personali 2015. Il Servizio ha curato l'*editing* dei testi ed il progetto grafico oltre che l'ideazione e la realizzazione della copertina.

È stata altresì curata l'edizione del nuovo volume cartaceo del Codice *privacy*, aggiornato alle più recenti innovazioni legislative.

È stato avviato il lavoro sulla nuova edizione aggiornata del *vademecum* dedicato alla tutela della *privacy* nella scuola per offrire indicazioni generali, tratte da provvedimenti, pareri e note del Garante riguardanti il delicato rapporto tra studenti, professori e famiglie, anche alla luce della nuova dimensione digitale.

Un altro apprezzato prodotto è stato il *vademecum* "*Privacy* e lavoro", con le regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati soprattutto con riferimento ai cartellini identificativi, bacheche aziendali, posta elettronica aziendale, controllo a distanza e geolocalizzazione dei lavoratori. La pubblicazione è stata realizzata nella sola versione digitale (a disposizione degli utenti sul sito istituzionale) ed è in programma una edizione aggiornata alla nuove regole introdotte dal *Jobs Act*.

Con un bassissimo costo in termini economici e utilizzando esclusivamente risorse interne, si è riusciti anche quest'anno a realizzare prodotti multimediali (provvedendo autonomamente alla scrittura e adattamento dei testi, sceneggiatura, sviluppo dell'animazione e selezione/costruzione degli elementi visivi, scelta delle musiche e sincronizzazione, registrazione dei testi, adattamento audio, montaggio e postproduzione). Sono state inoltre predisposte e diffuse nuove schede informative su varie tematiche, nuove pagine web e video.

La pagina dei "Consigli *flash*" si è arricchita di una nuova scheda su come tutelare la *privacy* con buone *password* (doc. web n. 4248578). Le schede *flash*, offrono spunti e orientamenti di base per tutelare i propri dati nella vita di tutti i giorni, con particolare attenzione all'uso delle nuove tecnologie. I suggerimenti proposti dalle schede invitano a riflettere su abitudini e comportamenti di cui ognuno di noi può fare tesoro per difendere la propria riservatezza.

È stata ideata e prodotta una campagna informativa dedicata alle *app* per *smartphone* e *tablet* intitolata "*App*-prova di *privacy*" corredata anche da un video *tutorial* divulgativo, ovvero un filmato di animazione che illustra le principali cautele da seguire quando si utilizzano applicazioni per *device* mobili e si vuole tutelare efficacemente la propria riservatezza. La campagna è stata integrata da azioni di comunicazione virale che hanno riscosso un deciso successo sui *social media*.

L'uso innovativo di tecniche di comunicazione virale è servito anche a riproporre, secondo il principio della "coda lunga", i numerosi materiali informativi e di comunicazione prodotti dal Garante nel corso del tempo. In particolare, sfruttando i canali *social*, sono stati ideari e diffusi *banner* grafici con immagini e *claim* che hanno permesso di riproporre e implementare l'attenzione e l'interesse per specifici contenuti nel corso del tempo, moltiplicando esponenzialmente la visibilità e il pubblico.

È stato progettato e lanciato il nuovo profilo del Gatante su Google+ (https://plus.google.com/u/1/+GarantedatipersonaliGP), che arricchisce la presenza *online* dell'Autorità, affiancandosi e integrandosi agli spazi di informazione e intera-

zione *social* già esistenti su Linkedin e Youtube. L'iniziativa ha permesso di ampliare il *target* di pubblico raggiunto attraverso i *social media*, intercettando anche un'utenza più generalista rispetto, a quella specialistica di Linkedin. Con riferimento a quest'ultimo *social media*, si segnala che nel 2015 i *followers* della pagina del Garante sono praticamente raddoppiati, raggiungendo circa 4.500 unità. Segno di un forte interesse per i contenuti proposti e per il canale di diffusione.

In vista della pubblicazione sulla GUUE del nuovo pacchetto protezione dati, è stata creata un'apposita pagina tematica sul sito del Garante (www.garanteprivacy/pacchettoprotezionedati), contenente notizie utili, aggiornamenti costanti, materiali di approfondimento, rimandi ai testi giuridici in elaborazione e un'infografica sulla figura del *privacy officer* (doc. web n. 4791352).

È stato implementato l'uso delle infografiche per semplificare la comprensione dei principali provvedimenti del Garante o di specifiche iniziative. In particolare, sono state predisposte infografiche per illustrare:

- il provvedimento recante le Linee guida sul *dossier* sanitario elettronico (doc. web n. 4101025);
- il processo di notificazione da parte dei soggetti che installano *cookie* su siti internet o *blog* (doc. web n. 4135757), adempimento previsto dal provvedimento dell'8 maggio 2014;
- gli esiti principali dell'indagine *Sweep day* 2015 svolta dagli esperti del Garante sull'internet dei bambini, per verificare in particolare se i principali siti internet visitati e alcune delle più diffuse *app* scaricabili su *smartphone* e *tablet* rispettano la *privacy* dei minori (doc. web n. 4242235).

Sono stati totalmente autoprodotti i progetti grafici di materiali (locandine, biglietti-invito, ecc.) necessari alla promozione e comunicazione dei principali eventi organizzati dal Garante.

Il sito del Garante si è arricchito di nuove sezioni (tra cui, la già cit. pagina sul pacchetto protezione dati e quella dedicata alla raccolta dei provvedimenti generali raccolti per aree tematiche e ordine cronologico), mentre numerose pagine e sezioni sono state ampliate e potenziate, tra le quali quella dell'Autorità trasparente (v. *amplius* par. 24.3).

23.4. *Le manifestazioni e le conferenze*

Giornata europea della protezione dei dati

Il 28 gennaio di ogni anno ricorre la Giornata europea della protezione dei dati personali. A partire dal 2007 questo è il giorno scelto per ricordare in tutta Europa l'adozione della convenzione di Strasburgo n. 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato dei dati. È una iniziativa promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte la Autorità preposte alla prorezione dei dati personali nei Paesi europei, istituita con l'intento di informare i cittadini sui diritti legati alla tutela della vita privata e delle libertà fondamentali. Nel 2015 il Garante italiano, per celebrare la IX Giornata europea, ha organizzato il convegno dal titolo "Il pianeta connesso. La nuova dimensione della *privacy*". I lavori sono stati aperti da Antonello Soro, presidente dell'Autorità Garante, e chiusi da Marina Sereni, vicepresidente della Camera dei deputati. Oltre ai componenti dell'Autorità Augusta Iannini, Giovanna Bianchi Clerici, Licia Califano – autorevoli relatori quali Juan Carlos De Martin (Politecnico di Torino); Antonio Spadaro (Civiltà Cattolica); Luca De Biase (Il Sole 24 Ore); Roberto Baldoni (Università di Roma La Sapienza); Massimo Russo (Wired Italia); Lella Mazzoli (Università di Urbino Carlo Bo); Giovanni Boccia Artieri (Università di

Urbino Carlo Bo); Andrea Granelli (Kanso); Federico Maggi (Politecnico di Milano), sono stati chiamati a discutere sulla difesa dei diritti delle persone nella nuova dimensione dell'infosfera quale *habitat* popolato di dati, informazioni ed esperienze condivise. Al riguardo il presidente Soro nel discorso di apertura ha affermato "Nella società digitale, noi siamo i nostri dati: da questa considerazione bisogna partire per cercare nuove e più efficaci forme di tutela delle nostre libertà. Seguire il percorso dei dati e la possibilità di mantenere il controllo sul flusso di informazioni che ci riguardano diventa sempre più complesso. L'interazione automatica tra gli oggetti permette una continua raccolta e condivisione di informazioni, senza alcuna consapevolezza delle persone cui le stesse appartengono". Secondo Soro "la protezione dei dati può rappresentare l'antidoto contro ogni possibile abuso, una risposta all'avanzare della società sorvegliata, il presupposto essenziale per garantire anche la sicurezza dei sistemi". "L'ambizione delle Autorità di protezione dati – ha concluso Soro – è quella di ricercare un nuovo equilibrio tra fattibilità tecnica ed accettabilità giuridica; di incorporare la tutela dei diritti nelle tecnologie e di responsabilizzare i titolari spingendoli verso l'adozione di nuovi modelli organizzativi di gestione e di controllo dei dati".

Ad ascoltare il dibattito sono stati invitati, tra gli altri, anche gli studenti di due licei di Roma: Liceo classico Augusto e Liceo scientifico Volterra. I testi di tutti gli interventi sono stati raccolti nel volume Il pianeta connesso.

Altri convegni

Tra i numerosi convegni ed incontri ai quali il presidente Soro ha partecipato nel corso dell'anno, molti sono stati legati alle tematiche della sicurezza dei dati personali nello spazio digitale o della sorveglianza di massa ai fini del contrasto al terrorismo. Intervenendo a Milano al *Wired Next Fest* (21-24 maggio), il presidente ha detto: "Il confine *online-offline* è crollato, tutelarsi in rete serve a vivere più sicuri nel mondo reale, e viceversa". "Se *online* – ha ribadito Soro – mettiamo a rischio le informazioni che ci riguardano, in sostanza la nostra vita, gli effetti si faranno sentire anche e soprattutto *offline*".

Il 21 ottobre si è svolto il 5° *Privacy day forum* organizzato da Federprivacy in occasione del quale il presidente Soro, in merito al rapporto tra protezione dei dati e mondo connesso, ha affermato che "Le possibilità offerte dalle tecnologie, la relazione sempre più stretta tra uomo e macchina e la sorveglianza diffusa hanno aumentato in modo esponenziale le potenzialità di erosione della nostra *privacy* e, quindi, della nostra libertà. Per questo il confronto sul futuro della *privacy* – si è augurato Soro –deve diventare in primo luogo una questione di sensibilità culturale e sociale: perché non possiamo rinunciare in nome del progresso tecnologico alla tutela dei diritti e dei princìpi su cui si fonda la nostra società: dignità della persona, reputazione, identità".

Diversi anche i convegni ai quali hanno partecipato i componenti del Collegio.

Il 28 marzo, nell'ambito dell'assemblea annuale dell'Ordine dei giornalisti della Sicilia, Augusta Iannini, vicepresidente del Garante, è intervenuta al convegno "Quando l'informazione non è minore – Cogne, Rignano, Avetrana, Santa Croce: avanti il prossimo" svoltosi a Santa Croce Camerina, in provincia di Ragusa. La vicepresidente ha affermato che "il rapporto tra *media* e minori è pieno di criticità irrisolte: i princìpi contenuti nella Carta di Treviso sono chiaramente indicati, ma la loro applicazione è deludente nonostante il diritto alla riservatezza sia sovraordinato al diritto di cronaca. L'interesse pubblico ad essere informati può essere rispettato garantendo l'anonimato dei minori nel rispetto della dignità della persona".

Sempre in tema di diritto di cronaca e *privacy*, Licia Califano, componente del Collegio, è intervenuta al convegno "La televisione del dolore, un'indagine sulle 'cattive pratiche' televisive" (Roma, 24 marzo), sostenendo che " il diritto alla riser-

vatezza e alla protezione dei dati personali rappresenta ormai stabilmente un diritto della personalità e un limite legittimo alla libertà di espressione".

Nell'ambito della XXXII Assemblea Annuale dell'Anci, svoltasi a Torino, il Garante ha organizzato il convegno "Nuove tecnologie e cittadino protetto. Una sfida per i Comuni 2.0. Videosorveglianza, *smart city*, sicurezza, *privacy officer*" (29 ottobre) i cui lavori sono stati aperti da Licia Califano.

Il 19 novembre a Roma si è svolta l'annuale edizione dell'evento organizzato da *Consumer's Forum* nel corso del quale è stato presentato l'ottavo rapporto annuale "Il consumatore nell'era della condivisione". All'incontro hanno partecipato le maggiori Autorità indipendenti e di settore per discutere della tutela dei diritti dei cittadini. Per il Garante è intervenuta la vicepresidente Augusta Iannini la quale sostenuto l'importanza di "sviluppare nei nuovi 'consumatori digitali' la consapevolezza dei rischi e delle opportunità che questo nuovo *habitat* digitale nel quale tutti ci muoviamo può comportare", sottolineando la necessità di "definire strategie integrate tra tecnologia e norma giuridica".

Giovanna Bianchi Clerici, componente del Collegio, a novembre, ha partecipato al convegno sul tema del "Diritto all'oblio, Carta di Treviso, *privacy*: la deontologia nel web" – dove ha ricordato gli effetti della sentenza cd. Google Spain della CGUE e i criteri che hanno guidato il Garante nel decidere sui ricorsi presentati dai cittadini italiani dopo il rifiuto opposto dalla società di Mountain View ad accogliere le loro richieste di deindicizzazione.

23.5. *Le relazioni con il pubblico*

Anche nel 2015, l'Ufficio relazioni con il pubblico ha svolto l'importante ruolo di primo punto di riferimento per tutti coloro che si sono rivolti all'Autorità utilizzando diverse modalità quali il telefono, le *e-mail*, la posta ed anche mediante visita in sede. L'Urp ha fornito informazioni su tutte le questioni attinenti alla protezione dei dati personali, da quelle connesse all'esercizio dei diritti riconosciuti alle persone fisiche, a quelle relative alle misure da adottare in materia di *cookies*, di trasferimento dei dari all'estero, di *telemarketing*, di trasparenza *online* della p.a., di sanità. Svolgendo la propria attività, incentrata sul riscontro all'utenza, sulla valutazione di novità ed "emergenze" e sull'informazione al cittadino, l'Urp continua ad essere il luogo di incontro tra l'Autorità e il pubblico, in un rapporto quotidiano ove i quesiti e le istanze di ciascuno sono oggetto di attenta e approfondita disamina.

Trova conferma, anche per l'anno di riferimento, la tendenza ad avvalersi in modo ripetuto dell'attività di supporto dell'Urp, istaurando con esso una sorta di relazione di "affidamento" e fiducia.

L'Ufficio svolge anche l'importante ruolo di collegamento tra le richieste degli utenti e gli interventi dell'Autorità, nonché quello di informazione a vantaggio delle altre unità organizzative mediante apposita reportistica interna, contribuendo a evidenziare le tematiche sulle quali maggiormente si concentra l'attenzione della società.

L'attività dell'Urp

A seguito dell'esame delle istanze ricevute, l'Ufficio valuta se al quesito possa essere dato immediato riscontro, attraverso il rinvio a provvedimenti già adottati dall'Autorità o se, invece, lo stesso debba essere trasmesso ad altre Unità. Le ulteriori attività riguardano la valutazione di novità ed "emergenze" di particolare rilevanza sociale o economica nonché l'informazione al cittadino, anche mediante la distribuzione di materiale divulgativo. Quest'ultima attività consente all'Autorità di realizzare la prima e più diretta diffusione della conoscenza della normativa in materia di protezione dei dati personali e dei valori alla stessa sottesi.

Anche nel 2015, sono stati realizzati strumenti diretti a migliorare l'offerta informativa del Garante in aggiunta alle modalità più tradizionali di informazione, nonché strumenti volti a consentire agli interessati di tutelare i propri diritti più semplicemente. In particolare, sono state predisposte delle FAQ in materia di trasparenza *online* della p.a. (doc. web n. 4519681), una dettagliata scheda informativa relativa ai ricorsi (doc. web n. 4539625) e un modello di reclamo *ex* art.142 del Codice (doc. web n. 4535524). L'attenzione dell'opinione pubblica nei confronti dell'attività del Garante è stata confermata dai dati statistici riguardanti l'attività dell'Urp, che hanno registrato nell'ambito dell'attività di *front office*, più di 25.500 contatti, la stragrande maggioranza dei quali avvenuti per via telefonica o per posta elettronica. In particolare, sono state ricevute 18.214 *e-mail* relative a segnalazioni, quesiti, richieste di informazioni e documentazione, alle quali l'Urp ha fornito, laddove possibile, riscontri immediati, svolgendo una preziosa e quotidiana attività di filtro e rimettendo agli altri uffici esclusivamente quelle istanze per le quali si è resa necessaria una più complessa attività istruttoria.

Gli affari definiti nel 2015 sono stati 432, mentre i visitatori ricevuti presso la sede dell'Ufficio sono stati 310 (cfr. sez. IV, tab 15).

Tematiche d'interesse

Molteplici sono state le questioni affrontate nel corso dell'anno (cfr. sez. IV, tab. 16), tra le quali si segnala ancora una volta quella del *telemarketing* aggressivo (5.871 *e-mail*), fenomeno ancora fonte, nonostante l'istituzione del Registro pubblico delle opposizioni, di grande disturbo per i cittadini, che lamentano la quantità e le modalità delle chiamate ricevute (numerose nell'arco della giornata e negli orari meno opportuni), ma anche l'insistenza e la scortesia degli operatori.

Frequentemente segnalate sono state l'attività di *marketing* svolta attraverso strumenti informatici (sms, fax e *e-mail*) e la ricezione delle cd. telefonate mute, questione che suscita particolare frustrazione per il fatto che l'interlocutore rimane silenzioso e il numero chiamante è il più delle volte oscurato (cfr. par. 11.1).

Molte richieste di intervento hanno riguardato l'attivazione di servizi a pagamento non richiesti sulle utenze di telefonia mobile, riserto alla quale il Garante ha da rempo in corso complessi accerramenti presso i diversi soggerri a vario titolo coinvolti nel fenomeno.

Costante si è mantenuto l'interesse degli utenti in materia di videosorveglianza, con particolare riferimento all'ambito condominiale, lavorativo e scolastico. In tale ultimo contesto, le tichieste hanno riguardato la possibilità di incrementare l'utilizzo delle videocamere in quegli istituti scolastici che si ttovano in situazioni particolarmente problematiche. Numerose sono state anche le richieste relative all'uso delle cd. *dashcam*, ossia sistemi di videoripresa montati, per scopi diversi, a bordo di veicoli.

Sempre alto è staro il numero delle segnalazioni e dei quesiti relativi ai trartamenti di dati personali nell'ambito dei rapporti di lavoro pubblico e privato (510 *e-mail*). Si segnalano, in particolare, oltre alle questioni legate all'utilizzo delle telecamere negli ambienti di lavoro, i temi connessi all'uso di internet e della posta elettronica sul posto di lavoro, al trattamento di dati sensibili correlato al riconoscimento di permessi o benefici, al controllo a distanza dei lavoratori mediante geolocalizzazione, al rilevamento delle presenze dei lavoratori mediante sistemi tecnologicamenre avanzati, *in primis* mediante l'uso di dati biometrici. Al riguardo, molte richieste hanno avuto ad oggetto il provvedimento generale prescrittivo in tema di biometria 12 novembre 2014, n. 513 (doc. web n. 3556992).

Confermato anche nel 2015 il grande interesse per il trattamento dei dati personali nell'ambito dei *social network*, ove in maniera non sempre consapevole gli individui, sopratturto giovanissimi, riversano grandi quantità di informazioni personali

e perfino di natura sensibile. Le difficoltà nascono nel momento in cui si intenda recuperare il controllo sulle informazioni precedentemente condivise e si decida, ad esempio, di cancellarle dalla piattaforma. Tale operazione non è sempre di agevole realizzazione, sia per le caratteristiche dei *social network*, nei quali peraltro si registrano variazioni delle condizioni d'uso del servizio decise spesso unilateralmente dai gestori dello stesso, sia per i limiti di applicabilità della normativa italiana rispetto a trattamenti di dati effettuati da titolati spesso aventi sede all'estero.

La sentenza della CGUE Google vs Spain, 13 maggio 2014(C-131/12), ha continuato a produrre importanti effetti, determinando un notevole incremento delle richieste di chiarimento e di intervento, in particolare volte ad ottenere la deindicizzazione dei contenuti personali dalla rete.

Immutato è stato altresì l'interesse per il tema relativo alla protezione dei dati e giornalismo, con riferimento alla corretta gestione dei cd. archivi storici *online* dei quotidiani, anche alla luce delle indicazioni fornite dalla Corte di Cassazione (III sez. civ., sentenza 05.04.2012, n. 5525).

L'opinione pubblica si è mostrata sempre molto attenta ai delicati temi concernenti il rapporto tra la tutela dei dati personali e l'esercizio della libertà di manifestazione del pensiero, nonché della divulgazione di immagini fotografiche, spesso riguardanti minori, sul web. Molte sono state le richieste di intervento e i quesiti che hanno riguardato in particolare la questione del bilanciamento del diritto alla protezione dei dati personali con il diritto di cronaca.

Un consistente numero di richieste ha avuto ad oggetto gli adempimenti relativi all'uso dei cd. *cookie*, in special modo nel periodo a ridosso della scadenza (2 giugno 2015) del termine per l'adozione delle misure prescritte nel provvedimento 8 maggio 2014, n. 229 (doc. web n. 3118884). Profili oggetto di maggiore attenzione sono stati: l'obbligo di realizzare il *banner* previsto dal provvedimento nel caso in cui si utilizzino soltanto *cookies* "tecnici"; il rapporto tra gestore del sito e cd. terze parti; la gestione dei *cookie* analitici di terze parti; la disciplina applicabile ai siti gestiti da soggetti *extra* UE; l'obbligo di notificazione al Garante. Data la delicatezza della tematica, il Garante ha fornito chiarimenti volti a semplificare il più possibile l'attuazione delle previsioni di legge, nonché a fornire la massima assistenza all'utenza. A tale scopo, in particolare, sono stati realizzati un documento contenente "Chiarimenti in merito all'attuazione della normativa in materia di *cookie*" (doc. web n. 4006878), nonché una scheda "infografica" sugli adempimenti. È stato inoltre organizzato un seminario formativo, tenutosi il 3 luglio presso il Centro di formazione della difesa (doc. web n. 4035684). Sempre numerose sono state altresì le richieste riguardanti i trattamenti di dati personali effettuati da soggetti pubblici per finalità di pubblicità e trasparenza sul web di cui al d.lgs. n. 33/2013. Accanto ai profili già emersi lo scorso anno (obbligo di pubblicazione dei redditi e dei dati patrimoniali di sindaci, consiglieri e assessori comunali, provinciali e regionali; modalità di pubblicazione degli elenchi di soggetti beneficiari di sovvenzioni o contributi; pubblicazione nell'albo pretorio di determine indicizzate in rete), oggetto di particolare attenzione sono state le pubblicazioni di atti contenenti dati riferiti alla condizione di disabilità dei partecipanti a concorsi e selezioni pubbliche.

Sempre significativa, in termini numerici, è la voce relativa alle richieste di informazioni degli utenti sugli adempimenti e sugli strumenti di tutela previsti dal Codice (1.424 *e-mail*), con particolare riferimento alle modalità con le quali attivare i predetti strumenti (segnalazioni, reclami e ricorsi).

Parimenti costante è stata l'attenzione al tema della protezione dei dati personali nell'ambito dei sistemi di informazioni creditizie, nonché alle questioni attinenti alla possibilità di accedere ai dati bancari invocando la normativa in materia di pro-

tezione dati, in contrapposizione al diritto di ottenere copia della documentazione bancaria sulla base dell'art. 119, d.lgs. n. 385/1993 (t.u. delle leggi in materia bancaria e creditizia). Quanto all'attività di recupero del credito, le questioni maggiormente segnalate sono state quelle relative alle modalità utilizzate per contattare i debitori e sollecitare i pagamenti, quali visite al domicilio o sul luogo di lavoro del debitore, sollecitazioni telefoniche non solo presso i suoi recapiti, ma anche presso familiari, vicini di casa, datori di lavoro, tutte non rispondenti alle misure indicate da tempo dal Garante.

Successivamente alla recente sentenza della CGUE 6 ottobre 2015 (C-362/14) concernente la causa che ha visto contrapposti il cittadino austriaco Maximillian Schrems e l'Autorità irlandese per la protezione dei dati in un caso relativo a Facebook, hanno avuto un notevole incremento le richieste di chiarimenti concernenri i trasferimenti di dati all'estero e il cd. accordo *Safe Harbor*. L'attenzione dei richiedenti si è concentrata, in particolare, sugli altri strumenti previsti dalla normativa per effettuare leciti trasferimenti di dati personali all'estero, quali ad es., le clausole contrattuali *standard* o le regole di condotta adottate all'interno di un medesimo gruppo (le cd. Bcr, *Binding corporate rules*).

24 Studi, documentazione e trasparenza

24.1. *Il Servizio studi e documentazione*

Predisposizione della Relazione annuale

Il Servizio studi ha coordinato la predisposizione del testo della Relazione annuale 2014: essa, oltre a costituire un importante adempimento (previsto dall'art. 154, comma 1, lett. *m*), del Codice), in ragione della completezza nella rappresentazione dell'attività (provvedimentale e non) dell'Autorità nell'anno solare di riferimento, costituisce un effettivo esercizio di trasparenza in relazione all'attività svolta, rendendone pienamente edotti non solo i suoi destinatari naturali, Parlamento e Governo, ma pure la collettività.

Inoltre, grazie ai puntuali riferimenti contenuti nel testo, la Relazione rappresenta uno strumento conoscitivo prezioso per gli interlocutori istituzionali dell'Autorità (titolari del trattamento, operatori giuridici, ricercatori, etc.), che trovano concentrata in un'unica sede (immediatamente ed agevolmente accessibile) la memoria storica di quanto realizzato nell'anno solare di rifetimento. Arricchendo le informazioni di natura statistica e rendendo immediatamente percepibile e (per quanto possibile) "quantificabile" in schede di sintesi la multiforme attività svolta, si è altresì mirato a realizzare una comunicazione più immediata, dal punto di vista del lettore (oltre che a beneficio degli infomediari), dell'operato dell'Autorità, in particolare dell'attività provvedimentale, sanzionatoria e comunicativa nonché degli impegni assolti nel contesto europeo ed internazionale.

Attività di documentazione interna

Il Servizio ha altresì svolto sistematicamente attività di documentazione interna (in relazione a novirà normative, giurisprudenziali e dottrinali incidenti nel settore della protezione dei dati personali) ed effettuato studi ed approfondimenti sulle materie all'attenzione dell'Autorità (spesso funzionali all'istruttoria di provvedimenti di carattere generale) o su questioni comunque di interesse mediante note di approfondimento e *dossier* (assicurandone il costante aggiornamento).

Attività di studio

Ha inoltre fornito, a mezzo di atti interni, elementi di valutazione ai fini della formulazione dei pareti richiesti dalla Presidenza del Consiglio dei ministri e dal Dipartimento per i rapporti con il Parlamento per l'eventuale impugnazione davanti alla Corte costituzionale delle leggi regionali ritenute di dubbia conformità limitatamente alla materia della protezione dei dati personali (cfr. par. 3.5) e delle risposte agli atti di sindacato ispettivo (cfr. par. 3.3).

Formazione esterna

Il Servizio ha infine curato la formazione esterna in materia di protezione dei dati personali: ciò è avvenuto con l'organizzazione di un seminario dedicato al tema "*Cookie* e protezione dei dati personali. Il provvedimento del Garante 8 maggio 2014, n. 229 sull'individuazione delle modalità semplificate per l'informativa e la manifestazione del consenso per l'uso dei *cookie*" svoltosi in Roma il 3 luglio 2015 presso il Centro di formazione della difesa che ha visto la partecipazione di 120 persone.

Due ulteriori seminari sono stati dedicati al tema "Sistemi informativi in ambito sanitario e protezione dei dati personali. Il provvedimento del Garante del 4 giugno 2015, n. 331, Linee guida sul *dossier* sanitario elettronico", tenutisi il 2 ottobre e il 4 dicembre 2015, rispettivamente presso l'*Auditorium* del Ministero della salute e presso il Centro congressi dell'Università cattolica del Sacro Cuore di Roma, cui hanno assistito complessivamente 370 partecipanti.

24

24.2. *La biblioteca*

La biblioteca nasce nel 2001 e rappresenta un'articolazione della segreteria generale. Il suo compito istituzionale consiste nel raccogliere, organizzare, classificare con criteri bibliografici, conservare, gestire e valorizzare le pubblicazioni italiane e straniere attinenti alla disciplina della protezione dei dati nonché alle tematiche dei diritti e delle libertà fondamentali, della dignità, della riservatezza e della identità personale. Il patrimonio della biblioteca, costituito da ca. 24.000 titoli (con 15.000 volumi, 7.500 dei quali in lingua straniera), è arricchito da un "fondo" speciale, donato dal prof. Rodotà e incrementato nel corso del tempo, che raccoglie ca. 2.000 documenti di particolare pregio da un punto di vista storico e retrospettivo sui temi del diritto alla riservatezza in Italia e sul *right to privacy* nella tradizione giuridica anglo-americana; un altro "fondo" di ca. 400 titoli è stato donato dal cons. Buttarelli. Presso la biblioteca esiste inoltre un deposito di ca. 200 tesi italiane di laurea e di dottorato in materia di protezione dei dati. Dal 2004 sul sito web della biblioteca in intranet è consultabile il catalogo OPAC che contiene 5.393 monografie e 90 periodici. Le acquisizioni successive al 2004 vengono pubblicate in formato elettronico con bollettini quadrimestrali.

La biblioteca – ulteriormente valorizzata dal completamento della catalogazione in OPAC e dalla sua immissione in internet – è nata per supportare le attività di informazione, di ricerca e di studio dell'Autorità; i servizi all'utenza esterna sono pertanto complementari (anche in ragione delle risorse disponibili) rispetto a questo fine istituzionale. Nel contesto generale di prosecuzione della razionalizzazione della spesa, l'Ufficio ha dovuto completare l'attivazione della opzione di recesso della sala conferenze che ha interessato nel 2014 anche i locali della biblioteca. Il successivo spostamento di quest'ultima in altri spazi dell'Autorità ha ridotto ad un'unica sala di consultazione le tre sale originarie, con il successivo trasferimento in nuovi magazzini di ca. il 75% delle collezioni possedute (attualmente il pattimonio a vista risulta collocato su ca. 107 metri lineari rispetto ai ca. 225 metri lineari antecedenti, mentre le collocazioni nei magazzini, uno dei quali in locali esterni alla biblioteca, occupano ca. 375 metri lineari).

La biblioteca rappresenta una singolarità a livello italiano ed europeo sotto numerose angolazioni. Il Garante italiano risulta difatti unico nella UE ad avere istituito una biblioteca specialistica di grandi dimensioni sui temi della *privacy* e della protezione dei dati. La stessa politica delle acquisizioni, rivolta anche all'incremento del patrimonio sul piano storico e retrospettivo, ttamite interventi sul mercato libtatio internazionale dell'usato, assume un parricolare rilievo nel panorama delle istituzioni bibliotecarie. In termini di comparazione e per l'utilità dei riscontri statistici (aggiornati al 31 dicembre 2015), il sistema SBN cataloga con il vocabolo "*privacy*" nel titolo 1.155 documenti a stampa (1.069 monografie, +152 sul 2015, e 73 spogli), 695 dei quali in italiano (628 monografie); 161 monografie con la stringa di "protezione dei dati" nel titolo (+ 12 sul 2015); 169 monografie con l'espressione di *"data protection"* (+ 6 sul 2015); 344 monografie (273 in italiano) sotto il soggetto di "Diritto alla riservatezza" (rispettivamente + 5 e + 8 sul 2015). Il polo bibliotecario parlamentare cataloga sotto il soggetto "riservatezza (diritto)" 982 *records* (495 in italiano) (rispettivamente + 52 e + 33 sul 2015): 615 *records* (246 in italiano) la biblioteca della Camera dei deputati e 367 *records* (249 in italiano) la biblioteca del Senato. I *records* aventi il vocabolo *"privacy"* nel titolo sono 349 (206 in italiano, 115 alla Camera e 91 al Senato). In Germania, la Deutsche Nationalbibliothek conta 1.816 *records* (+ 117 sul 2015), dei quali 783 volumi, con ricerca sul vocabolo

"privacy" nel titolo e 2.885 volumi con ricerca sul vocabolo *"Datenschutz"* nel titolo. Negli Stati Uniti, la principale biblioteca giuridica mondiale, la Harvard Law School Library, cataloga sotto la voce onnicomprensiva *"privacy"* ben 171.597 titoli, dei quali 8.592 volumi (962 per il biennio 2014-2015). Sotto la stringa *"Data protection"* risultano 4.480 volumi; sotto la stringa *"Data protection - Law and legislation"* 1.148 volumi; sotto la stringa *"Data protection - Italy"* 80 volumi; sotto la stringa *"Data protection - Law and legislation - Italy"* 40 volumi (i risultati sulla *data protection* in lingua italiana sono limitati al periodo 1984-2010). Sotto il soggetto "*Privacy - right of*" figurano 17.788 *items*, dei quali 4.336 volumi. La *Yale Law School* sotto la stringa "*Privacy*" cataloga 3877 titoli; sotto la stringa "*Privacy - right of*" 2571 titoli; sotto la stringa "*Privacy - right of - Italy*" 80 titoli. Infine, la *Library of Congress* cataloga sotto il soggetto "*Privacy - right of*" 3.968 documenti; sotto il soggetto "*Privacy - right of - Italy*" 98 documenti; sotto il soggetto "*Data protection*" 4.401 documenti; sotto il soggetto "*Data protection - Italy*" 139 documenti.

Nel 2015 i servizi all'utenza interna ed esterna sono stati dapptima ridotti e poi nuovamente sospesi a causa degli impegni di organizzazione del secondo trasloco. A partire dal mese di ottobre i servizi sono stati progressivamente ripristinati. Questi i dati relativi agli utenti interni: 995 i documenti richiesti in lettura; 295 i prestiti; 850 le richieste di fotoriproduzioni; 72 i casi di assistenza bibliotecaria (26 *online*); 12 le riproduzioni di documenti con inoltro in formato elettronico. Questi i dati sul pubblico esterno: 12 le autorizzazioni alla frequentazione; 134 i titoli consegnati in lettura; 104 le richieste di fotoriproduzioni; 52 i casi di assistenza bibliografica *online*; 80 gli invii di *document delivery*. La consultazione del catalogo OPAC sulla intranet ha registrato 7203 contatti. Per quanto riguarda i database giuridici gestiti sulla intranet attraverso il sito web della biblioteca, i dati di consultazione da parte dei dipendenti dell'Autorità rivestono speciale importanza come indicatori dell'elaborazione che precede la messa a punto dei "prodotti" dell'Ufficio. Gli elaborati statistici indicano che il numero totale dei documenti consultati nel 2015 ha ampiamente superato il traguardo simbolico di ca. 100.000. Il *database* con il più elevato conteggio ha registrato 6.864 sessioni di lavoro (6.814 nel 2014, 6.529 nel 2013, 5.828 nel 2012, 4.889 nel 2011 e 4.052 nel 2010) e 75.147 documenti consultati (83.831 nel 2014, 75.525 nel 2013, 60.419 nel 2012, 60.141 nel 2011 e 48.112 nel 2010), per una media giornaliera lavorativa di ca. 30 connessioni e 326 documenti (30 connessioni e 364 documenti nel 2014, 28 connessioni e 337 documenti nel 2013). Il calo riscontrato nel *download* di documenti risulta compensato dall'incremento nel numero di accessi e consultazioni degli altri *database* giuridici specializzati.

24.3. *L'Autorità trasparente*

D.lgs. n. 33/2013 e Autorità indipendenti

Come segnalato nella Relazione 2014 (p. 189), la riformulazione dell'art. 11, d.lgs. n. 33/2013 ad opera dell'art. 24-*bis*, d.l. 24 giugno 2014, n. 90, convertito, con modificazioni, dalla l. 11 agosto 2014, n. 114, ha determinato l'applicazione integrale (e non più, quindi, "secondo le disposizioni dei rispettivi ordinamenti") della disciplina di trasparenza anche alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione.

Per il Garante, ciò ha determinato il superamento del regolamento n. 1/2013 concernente gli obblighi di pubblicità e trasparenza relativi all'organizzazione e all'attività dell'Autorità (delibera 1° agosto 2013, n. 380, doc. web n. 2573442)

e della delibera 17 ottobre 2013, n. 455 (doc. web n. 2753146), recante la Disciplina dei periodi di tempo di pubblicazione di dati, informazioni e documenti del Garante per la protezione dei dati personali, strumenti attraverso i quali il Garante aveva dato prima attuazione alla disciplina sulla trasparenza amministrativa.

Le principali novità in materia di trasparenza presso il Garante

La ricordata modifica normativa dell'art. 11, comma 1, d.lgs. n. 33/2013, ha quindi reso urgente una riconsiderazione nel corso del 2015 – tenendo conto delle esigue risorse disponibili presso l'Autorità destinate a tale compito, considerata l'ampiezza dei compiti istituzionali attribuiti al Garante e del suo limitato organico – della struttura (*layout*) e dei contenuti della sezione "Autorità trasparente". Tale attività, realizzata nel primo semestre per il tramite di un'approfondita ricognizione realizzata dal responsabile della trasparenza, designato con provvedimento 22 gennaio 2015, n. 29 (doc. web n. 3732817), ha trovato progressiva attuazione nella seconda parte dell'anno, da un lato, con la revisione della struttura complessiva del sito istituzionale dell'Autorità, in conformità del vigente quadro normativo e tenendo conto delle indicazioni fornite dall'Anac; dall'altro, con l'aggiornamento ed una più opportuna dislocazione dei contenuti già esistenti nella sezione "Autorità trasparente", integrandone gli elementi carenti e potenziandone qualità e fruibilità.

A tali esiti è stato possibile pervenire, oltre che in ragione della menzionata ricognizione, grazie alle attività poste in essere dalle unità organizzative dell'Autorità, anche tramite l'operato di referenti per la trasparenza.

All'esito di tali complessive attività, il Garante ha infine adottato, con provvedimento 17 dicembre 2015, n. 659 (doc. web n. 4538976), sia misure organizzative interne, contenute nelle Procedure per l'adempimento degli obblighi di pubblicazione previsti dal d.lgs. n. 33/2013 presso il Garante, sia l'Aggiornamento 2015 del Programma triennale per la trasparenza e l'integrità 2014-2016, redatto sulla base delle indicazioni contenute nella delibera della Civit (ora Anac) n. 50/2013, recante Linee guida per l'aggiornamento del Programma triennale per la trasparenza e l'integrità 2014-2016.

Perfezionamenti della sezione Autorità trasparente, con particolare riferimento alla veste grafica con la quale dati e informazioni sono pubblicate, al fine di renderne più agevole ed immediata la fruizione – concentrando in un unico spazio, in maniera coerente, chiara e sintetica, le informazioni pertinenti – potranno essere introdotti nel 2016. In questa prospettiva, infatti, oltre che per realizzare economie di spesa, l'Autorità ha già provveduto ad acquisire il *software* per la gestione dei flussi informativi e documentali preordinati a realizzare la trasparenza amministrativa messo a disposizione da AgID per il riuso da parte delle pp.aa., il cui effettivo utilizzo richiede tuttavia alcune necessarie "personalizzazioni" per renderlo coerente con la diversa natura e struttura organizzativa propria del Garante.

Seminari e convegni su trasparenza

L'attenzione del Garante rispetto alle tematiche della trasparenza amministrativa non si è tuttavia esaurita nel dare piena attuazione alla disciplina contenuta nel d.lgs. n. 33/2013. Come già avvenuto in passato, il Garante ed il personale dell'Ufficio hanno continuato a svolgere un ruolo attivo nella trattazione delle tematiche legate alla trasparenza amministrativa, sia nello svolgimento dei propri compiti di controllo, ma anche prendendo parte a seminari ed incontri incentrati sul tema e sul corretto contemperamento delle misure volte ad attuare la trasparenza amministrativa con i diritti fondamentali delle persone, con particolare riferimento alla riservatezza e al diritto alla protezione dei dati personali. In questa prospettiva deve essere letto il ruolo attivo svolto dal Garante anche nella forma della partecipazione a convegni ed iniziative formative: tra questi, possono qui ricordarsi gli interventi della vicepresidente Augusta Iannini nell'ambito delle "Giornate della trasparenza" a

Potenza e Matera (12 e 13 gennaio 2015) e all'analoga iniziativa, incentrata su "La trasparenza nelle pubbliche amministrazioni tra apparenza, percezione e effettività", tenutasi presso il Consiglio regionale del Lazio il 1° dicembre 2015; e ancora, la partecipazione della professoressa Licia Califano, tra gli altri, al convegno organizzato il 30 gennaio 2015 dalla Scuola di specializzazione in studi sull'amministrazione pubblica – Università degli studi di Bologna "Trasparenza vs *Privacy*: Due diritti compatibili? Una riflessione dopo il d.lgs. 33 del 2013" e ad analoga iniziativa promossa dall'Università Carlo Bo "Anticorruzione, trasparenza e *privacy*: la dimensione costituzionale e le regole del bilanciamento" tenutasi il 15 aprile 2015 a Utbino.

PAGINA BIANCA

L'Ufficio del Garante

PAGINA BIANCA

III - L'Ufficio del Garante

25 La gestione amministrativa e dei sistemi informatici

25.1. *Il bilancio e la gestione finanziaria*

Il Garante ha continuato ad utilizzare nel 2015 un sistema di contabilità finanziaria basato su princìpi di programmazione della spesa e di prudente valutazione delle entrate.

La gestione amministrativa è stata improntata al pieno rispetto delle disposizioni legislative e regolamentari applicabili all'Autorità in materia contabile e di riduzione della spesa. Per effetto delle decisioni assunte nel corso dell'anno, che hanno tenuto conto anche dei vincoli legislativi introdotti dalle specifiche norme di legge vigenti, si è conseguito un lieve *surplus* di bilancio che denota una gestione improntata al sostanziale equilibrio finanziario. Infatti, anche se nel 2015 si è registrata una contrazione delle entrate rispetto al precedente esercizio (-8,24%), il risultato della gestione di competenza è stato positivo in valore assoluto per 0,5 milioni di euro e la relativa misura è ascrivibile ad una attenta politica di contenimento delle spese che ha determinato una contrazione degli oneri, sia rispetto alle originarie previsioni, sia riguardo ai dati relativi al precedente esercizio finanziario.

Il sostenimento degli oneri di funzionamento dell'Autorità sono posti a carico delle risorse erariali in ragione delle peculiarità dei compiti istituzionali del Garante, i cui ambiti di competenza non consentono di individuare agevolmente specifici operatori di settore su cui poter far gravare quota parte degli oneri di funzionamento, secondo modalità analoghe a quelle già vigenti nel nostro ordinamento in favore di numerose autorità indipendenti. Tale situazione rischia di rendere difficoltoso definire un contesto normativo che assicuri un sostanziale autofinanziamento e che affranchi l'Autorità dalla necessità di far gravare le proprie spese di funzionamento anche sulla fiscalità generale. Ne consegue che resta di stringente attualità per il Parlamento valutare l'adozione di specifiche ed idonee misure che consentano al Garante l'acquisizione delle risorse finanziarie necessarie all'effettivo esercizio delle proprie funzioni, nel rispetto delle prescrizioni poste dalle competenti Istituzioni comunitarie in capo ai singoli Stati membri dell'UE.

Le entrate ascrivibili all'autofinanziamento sono costituite in massima parte da sanzioni irrogate dal Garante nell'ambito delle verifiche previste dal Codice e, in misura meno rilevante, da diritti di segreteria. In ogni caso la loro entità risulta marginale rispetto alle complessive risorse finanziarie occorrenti ad assicurare il corretto funzionamento dell'Ufficio. Sotto il mero profilo delle risultanze contabili registrate nel 2015 (cfr. sez. IV, tab. 19), l'Ufficio ha potuto fare affidamento su entrate complessive pari a 19,2 milioni di euro, delle quali l'entità più significativa, ammontante a 10,0 milioni di euro, è rappresentata dai trasferimenti di natura straordinaria assicurati da altre autorità indipendenti in base ad un puntuale obbligo legislativo. Va soggiunto, tuttavia, che tali specifici trasferimenti, ammontanti ad oltre il 50% delle effettive necessità finanziarie complessive, terminano con l'anno 2016 e, laddove non adeguatamente reintegrate, sono destinate a lasciare l'Autorità in una prospettiva di potenziale *deficit* strutturale già a

decorrere dall'esercizio finanziario 2017. Infatti, i trasferimenti erariali, che in passato costituivano l'entità pressoché esclusiva delle fonti di finanziamento del Garante, nel corso degli anni si sono progressivamente ridotti e nel 2015 sono stati pari a 6,9 milioni di euro (il 35,73% delle entrare totali), importo in flessione rispetto al precedente esercizio (-9,78%). L'equilibrio di bilancio è stato raggiunto solo grazie al concorso dei trasferimenti, di natura provvisoria, operati proprio dalle altre autorità indipendenti. Le ulteriori e residuali entrate acquisite al bilancio nel corso dell'anno sono state pari a 2,3 milioni di euro, il cui importo deriva in misura prevalenre dalla quota di sanzioni amministrative comminate dall'Autorità. Le entrate acquisite nel corso dell'anno sono srate utilizzate per fare fronte agli oneri obbligatori, connessi allo svolgimento dei compiti istituzionali ed al perseguimento degli obiettivi programmatici definiti in sede di approvazione del bilancio di previsione. L'utilizzo di tali risorse finanziarie è avvenuto nel rispetto delle indicazioni legislative valide per la generalità dei soggetti pubblici e per le autorità amministrative indipendenti in particolare. Nel 2015, infatti, il Garante ha dovuto tenere conto, tra i diversi obblighi vigenti in materia di spesa pubblica, dei vincoli previsti espressamente dall'art. 22, d.l. n. 90/2014, convertito, con modificazioni, dalla l. n. 114/2014. Una prima prescrizione ha riguardato la riduzione del trattamento economico accessorio del personale dipendente, inclusi i dirigenti. A tale obbligo l'Autorità ha adempiuto adottando una specifica delibera, volta al contenimento della spesa, a cui è srara data tempestiva applicazione. Ulteriori misure previste dalla legge sono ascrivibili alla necessità di ridurre di almeno il 50% la spesa per incarichi di consulenza, studio o ricerca. La disposizione in questione non ha interessato il Garante per la prorezione dei dati personali in qnanto nel 2015 l'Autorità non ha conferito alcun incarico e, quindi, non ha sostenuto alcun onere per tale tipologia di spesa.

Dal raffronto dei dati consuntivi dell'esercizio con quelli dell'anno precedente emerge una contrazione della spesa totale del 2%. Infatti, a fronte di oneri complessivi del 2014 per 19,1 milioni di euro, il 2015 ha fatto registrare una spesa totale di 18,7 milioni di euro. Con specifico riferimento alle ulteriori norme di *spending review*, adotrate dal legislatore nel corso degli anni ed applicabili anche nel 2015, l'Autorirà si è sempre prontamente adeguata affinché si perseguissero gli obiettivi di contenimento della spesa prefissati. In ragione di ciò, sono stati rispettati i limiti riguardanti gli oneri per consumi intermedi di cui all'art. 8, comma 3, d.l. n. 95/2012, convettito con modificazioni, dalla l. n. 135/2012.

Si è altresì adempiuto agli obblighi connessi alla gestione e all'esercizio di autoveicoli, nei termini previsti, da ultimo, dall'art. 5, comma 2, del medesimo d.l. n. 95/2012. In particolare, nell'evidenziare che l'Autotità non è proprietaria di alcuna autovettura, dalle risultanze contabili emerge che la spesa relativa alle esigenze istituzionali di mobilità è stata contenuta entto i pur ristretti limiti di legge.

La dinamica complessiva della spesa, in conclusione, è risultara fortemente influenzata dalle misure di contenimento applicate e dagli obblighi contrattuali connessi all'espletamento delle peculiati funzioni istituzionali demandate al Garante dal Codice e dalla legislazione comunitaria, quest'ultima sempre più stringente quanto ad incombenze poste a carico delle autorità nazionali in materia di tutela delle persone fisiche con tiguardo al trattamento dei dati personali e alla libera circolazione di tali dati.

25.2. *L'attività contrattuale e la gestione economale*

L'attività contrattuale dell'Autorità, si è svolta in attuazione degli obiettivi generali fissati dal Garante, continuando a perseguire le finalirà di miglioramento in termini di efficienza e risparmio. Tale attività è stata anche influenzata dalle riforme normative del 2014 riguardanti i servizi da gestire in comune con le altre autorità amministrative indipen-

denti. Tra le varie innovazioni introdotte dal d.l. n. 90/2014, poi convertito in legge, con modificazioni, dall'art. 1, comma 1, della l. n. 114/2014, è stato stabilito (art. 22, comma 7) che le autorità indipendenti gestiscano "i servizi strumentali in modo unitario, mediante la stipula di convenzioni o la costituzione di uffici comuni ad almeno due organismi". Al fine di dare applicazione a tale previsione normativa, dopo diversi incontri con altre autorità potenzialmente interessate, in data 17 dicembre 2014 è stata sottoscritta una convenzione fra Autorità per le garanzie nelle comunicazioni, Autorità per l'energia elettrica il gas e il sistema idrico e il Garante, con la quale si è deciso di avviare la prevista collaborazione nella gestione dei servizi relativi ad affari generali, acquisti e appalti ed amministrazione del personale, con l'obiettivo di perseguire i risparmi richiesti dalla legge. Nel 2015 si sono susseguite quindi diverse riunioni, finalizzate a valutare i vari aspetti propedeutici all'esercizio in comune delle predette funzioni. In particolar modo, la verifica ha preso in considerazione la possibilità di espletare congiuntamente talune procedure di gara, richiedendo la predisposizione di specifici documenti di approfondimento e la messa in comune del relativo patrimonio informativo, per valutare contenuti e tempi di realizzazione di eventuali azioni congiunte. In corso d'anno tale elaborazione si è arricchita dell'apporto di Consip S.p.A. che, proprio sulla base dei lavori portati innanzi dalla convenzione, ha istituito un tavolo comune fra tutte le autorità indipendenti volto a verificare la possibilità di predisporre procedure di gara coordinate dalla propria struttura. Al termine del 2015 le tre autorità, originali firmatarie della convenzione sopra menzionata, hanno deliberato l'adesione alla stessa da parte dell'Autorità di regolazione dei trasporti, che aveva rivolto specifica istanza in tal senso.

Per quanto riguarda il conseguimento dei richiesti risparmi, anche attraverso una razionalizzazione delle risorse esistenti, il Garante ha proceduto, nella seconda metà dell'anno, ad accorpare i servizi relativi alla gestione delle risorse umane, all'attività contrattuale ed alla gestione dell'immobile e alla formazione in un'unica unità organizzativa, denominata Dipartimento risorse umane e strumentali, con conseguente soppressione di due posizioni dirigenziali e possibili ulteriori sinergie nell'ambito delle risorse assegnate al "nuovo" dipartimento.

Fra le ulteriori novità normative aventi effetto sul settore considerato devono essere richiamati l'art. 1, comma 450, l. n. 296/2006, così come integrato dall'art. 22, comma 8, lett. *b*), d.l. n. 90/2014, che ha esteso anche alle autorità indipendenti alcuni obblighi relativi alla utilizzazione della piattaforma Consip S.p.A. (in particolare rendendo obbligatorio il ricorso al Mercato elettronico della pubblica amministrazione, fermi restando gli ulteriori, previgenti obblighi); nonché, sotto altro profilo, l'art. 24-*bis*, d.l. n. 90/2014 che ha esteso gli obblighi di trasparenza previsti dal d.lgs. n. 33/2013, comportando l'implicito superamento del previgente regolamento dell'Autorità n. 1/2013 e costringendo l'Ufficio ad una nuova, generale revisione delle attività finalizzate alla corretta attuazione delle nuove disposizioni.

Per quanto specificamente attiene all'attività contrattuale, – anche in virtù di quanto previsto dalla normativa testé citata – si registra l'ulteriore aumento del ricorso alle forme di *e-procurement*, sia nella forma del cottimo fiduciario (Richiesta di Offerta) che nella forma dell'adesione alle Convenzioni stipulate da Consip S.p.A., sia nella forma dell'ordine diretto al miglior offerente, quest'ultima con riferimento a contratti di importo contenuto (cd. micro-conttattualistica). A tal proposito si evidenziano, tra le procedure comparative, quelle che hanno condotto alla stipula di un nuovo contratto triennale di fornitura di toner per stampanti, di un contratto avente ad oggetto un ampio programma di formazione – sia di medio livello che di livello specialistico – riguardante la lingua inglese e, infine, di un nuovo contratto triennale di fornitura dei servizi di stampa dei ptodotti editoriali del Garante. Può essere utile sottolineare che la media dei ribassi conseguiti nelle procedure di Richiesta di Offerta

– utilizzate, come negli anni ptecedenti, anche in presenza di impotti stimati di spesa molto inferiori al limite normativo pari a 40.000,00 euro – si è collocata al di sopra del 20%. Tra le adesioni alle Convenzioni Consip, si evidenzia invece quella relativa alla fornitura di energia elettrica, mentre per quanto concerne gli ordini diretti al miglior offerente si segnala che il ricorso a tale procedura è stato minimizzato sia nel numero (n. 18 ordini) che nell'importo medio (circa 1.100,00 euro) di ogni singolo acquisto, ben al di sotto delle soglie previste dalla normativa per gli affidamenti diretti.

Al di fuori dell'ambito di pertinenza di Consip S.p.A., meritano di essere menzionate le procedure di gara per l'affidamento dei servizi assicurativi relativi ai beni e all'attività istituzionale del Garante, che si concluderanno nei primi mesi del 2016, nonché la procedura comparativa relativa all'affidamento in concessione del servizio di cassa e tesoreria, che ha determinaro l'individuazione di un nuovo istituto bancario concessionario del servizio. Inoltre sono stati effettuati alcuni affidamenti diretti ai sensi dell'art. 57, comma 2, lett. *b)*, del codice dei contratti pubblici (cd. fornitore unico), tiguardanti principalmente la partecipazione dell'Autorità ad eventi di settore e l'acquisizione di ptodotti o servizi informatici necessari alla regolare prosecuzione delle attività dell'Ufficio quali la partecipazione all'assemblea nazionale Anci 2015, il rinnovo del servizio di accesso alle banche dati del sistema delle camere di commercio e la manutenzione del *software* relativo al sistema di protocollo informatico e gestione documentale.

Riguardo all'attività di carattere logistico ed economale, nella prima parte dell'anno si sono completate le procedure di restituzione, alla Società proprietaria della sede dell'Autorità, dell'ampia porzione locata corrispondente alla sala conferenze, oggetto di dismissione nel 2014. La maggior parte degli ulteriori interventi ha riguardato la manutenzione ordinaria degli impianri e alcune operazioni di risistemazione logistica del patrimonio librario dell'Autorità.

25.3. *Le novità legislative, regolamentari e l'organizzazione dell'Ufficio*

Nel 2015, è proseguita la rigorosa attuazione delle disposizioni previste dal d.l. n. 78/2010, convertito, con modificazioni, dalla l. n. 122/2010. In tale quadro, anche nel periodo considerato non sono stati conferiti incarichi di consulenza e, quanto alle auto di servizio, l'Autorità ha continuato a disporre esclusivamente della sola vettura di servizio, peraltro messa a disposizione dalla Guardia di finanza, per le esigenze di mobilità del Presidente. Al fine del conseguimento degli obiettivi di risparmio di cui all'art. 22 (Razionalizzazione delle autorità indipendenti), d.l. n. 90/2014, convertito, con modificazioni dalla l. n. 114/2014, nel 2015 sono stati avviati frequenti contatti fra le autorità coinvolte al fine di dare attuazione alla convenzione stipulata alla fine del 2014 tra Garante, Autorità per l'energia elettrica, il gas e il sistema idrico e Autorità per le garanzie nelle comunicazioni. La predetta convenzione è stata altresì estesa, a dicembre 2015, all'Autorità di regolazione dei trasporti.

Con tale convenzione, conformemente a quanto disposto dalla citata normativa, si è stabilito di procedere alla gestione in modo unitario dei servizi relativi ad "affari generali", "acquisti ed appalti" e "amministrazione del personale". In virtù di tale accordo, il Garante ha deciso di far convergere le attribuzioni del Dipartimento risorse umane e del Dipartimento contratti e risorse finanziarie in un nuovo Dipartimento risorse umane e strumentali, al quale sono state definitivamente affidate anche le competenze in materia di formazione del personale precedentemenre assegnate ad una specifica funzione. In questo modo si è registrata una riduzione delle risorse dirigenziali (da tre ad una) con conseguenti, sensibili risparmi di spesa, supetiori anche al limite posto dalla normativa richiamata.

Sotto lo specifico profilo dell'amministrazione del personale e della formazione, la prima fase di interlocuzione con le altre autorità ha mostrato alcune complessità legate alle diversità ordinamentali ed organizzative ma ha contestualmente lasciato intravedere un proficuo terreno di confronto e di scambio reciproco. Nel corso dell'anno, il lavoro si è concentrato sull'analisi dell'esistente e sull'individuazione di possibili, utili sinergie. In ral senso meritano di essere menzionati gli incontri con i rappresentanti di tutte le autorità amministrative indipendenti, indetti dalla Consip su specifico interessamento dei componenti della citata convenzione, volti ad esplorare la possibilità di avviare procedure unificate di selezione del contraente in materia di contratti assicurativi e di intermediazione assicurativa, con particolare riferimento all'assistenza integrativa ai dipendenti, nonché di procedure comuni di acquisto sul Mercato elettronico della p.a..

Nei primi giorni del 2015 è stata aperta alla firma anche la convenzione quadro in materia di procedure concorsuali per il reclutamento del personale delle autorità indipendenti ai sensi dell'art. 22, comma 4, del cit. d.l. n. 90/2014. Tale convenzione disciplina le procedure di informazione da seguire quando un'autorità intenda bandire un concorso e le regole per la gestione congiunta delle procedure allorché una o più autorità manifestino interesse alla copertura delle figure professionali oggetto del bando.

Sono state promosse da altre autorità alcune procedure concorsuali alle quali, tuttavia, il Garante, in ragione della specificità dei profili che venivano richiesti, non ha ritenuto di aderire. Pertanto, non vi è stato incremento di personale, mentre, analogamente all'anno precedente, dopo aver apportato alcune innovazioni alla disciplina di competenza dell'Autorità, sono state espletate due procedure per la selezione, complessivamente, di n. 10 stagisti (n. 5 per semestre). Con provvedimento 25 giugno 2015, n. 374 (doc. web n. 4078191) sono state approvate alcune modifiche al regolamento n. 1/2000 sull'organizzazione ed il funzionamento dell'Ufficio del Garante. In particolare, oltre ad aggiornare alcuni riferimenti normativi, si è rivista l'organizzazione dei dipartimenti e dei servizi, accorpando alcune funzioni in un'ottica di riduzione della spesa e di maggiore efficienza operativa e si è contestualmente meglio disciplinata la possibilità di istituire al loro interno unità di secondo livello. La durata di tutti gli incarichi di direzione, di primo e di secondo livello (ad eccezione di quelli per i quali è richiesta una professionalità specifica), è stata fissata in due anni rinnovabili per una sola volta. Infine è stata rivista la disciplina per gli incarichi di diretta collaborazione del Presidente e dei Componenti del Collegio, destinando a tale funzione, almeno in via prioritaria, il contingente di posti a contratto a tempo determinato ridotto ad otto unità in virtù delle modifiche introdotte dall'art. 1, comma 268, della l. n. 147/2013.

È stato poi siglato un importante accordo con la Polizia di Stato, in base al quale, in un'ottica di collaborazione tta amministrazioni e di scambio di competenze e di esperienze di interesse specifico, il Garante si è impegnato ad ospitare per un periodo della durata massima di due anni, presso la propria struttura organizzativa, due funzionari con profilo informatico appartenenti ai ruoli della polizia postale. Tale personale sarà formato ed impiegato in attività idonee a sviluppare un'esperienza specifica in materia di applicazione della protezione dei dati, anche in visra dell'emanando regolamento europeo.

Nel 2015 è stata poi stipulata una convenzione con la Scuola nazionale di amministrazione (Sna) in base alla quale, avendo messo a disposizione i docenti per i corsi in materia di protezione dei dati personali, è stata consentira la partecipazione gratuita dei dipendenti dell'Autorità ai seminari da questa organizzati.

Da segnalare, infine, l'implementazione delle misure di sicurezza previste dal d.lgs. n. 81/2008 in materia di sicurezza sui luoghi di lavoro, mediante la prosecu-

zione delle attività ordinarie e la costituzione e formazione degli organi previsti.

Servizio di segreteria del Collegio

Il Servizio di segreteria del Collegio ha curato nel corso dell'anno gli adempimenti necessari allo svolgimento delle attività di tale organo e in particolare: predisposizione e distribuzione della documentazione necessaria per le riunioni del Collegio, conservazione dei verbali delle riunioni e degli originali delle deliberazioni adottate nonché del materiale utile per la pubblicazione in Gazzetta Ufficiale.

Inoltre il Servizio, in stretto raccordo con le diverse articolazioni dell'Ufficio, ha provveduto all'attento controllo dei testi deliberati dal Collegio e ha contribuito – tramite la redazione web – all'attività di pubblicazione degli stessi sul sito istituzionale dell'Autorità. Peraltro, ha provveduto a curare l'implementazione e l'aggiornamento della sezione dedicata al Servizio nell'area intranet dell'Autorità. Anche nel 2015, conformemente a quanto disposto dall'art.15 del regolamento n.1/2000 e nel rispetto del Cad, l'Autorità ha proseguito nell'utilizzo di modalità di trasmissione elettronica dei documenti predisposti per l'esame e l'approvazione da parte del Collegio, per assicurare maggiore celerità ed efficienza nonché la progressiva sostituzione del mezzo cartaceo con quello elettronico, con risparmio di costi e tempo nonché recupero di spazio. Si segnala anche la piena fruibilità, nell'area intranet, dei testi dei provvedimenti adottati dal Collegio, per i quali dal 2011 è stato improntato l'apposito registro interno delle deliberazioni collegiali. Il Servizio di segreteria peraltro ha contribuito a gestire le eventuali richieste di oscuramento dei dati personali pervenute all'Ufficio da parte degli interessati o dai titolari del trattamento coinvolti a vario titolo in alcune istruttorie condotte dall'Autorità, in particolare con riferimento a esigenze di riservatezza riguardo a casi di segreto industriale o *know out* tecnologico.

25.4. *Il personale e i collaboratori esterni*

Con provvedimento 25 giugno 2015, n. 374 (doc. web n. 4078191) ed in conformità alle modifiche introdotte dall'art. 1, comma 268, della l. n. 147/2013 (legge di stabilità 2014) è stato portato a completamento, l'assetto relativo al personale a contratto, rinnovando n. 5 contratti a tempo determinato per il personale di diretta collaborazione dell'organo di vertice. Nel periodo di riferimento, si sono svolte due procedure per la selezione di 5 giovani laureati per l'effettuazione di periodi di tirocinio di sei mesi presso l'Autorità. Nel 2015, 10 giovani laureati hanno quindi svolto un periodo di formazione e orientamento presso il Garante. Sono cessate a vario titolo dal servizio n. 2 unità di personale di cui 1 con qualifica di dirigente e 1 di funzionario. Al 31 dicembre 2015 l'Ufficio poteva contare su una dotazione organica costituita complessivamente da 137 unità (di cui 111 in servizio), al quale va aggiunto un contingente di personale a contratto di 8 unità (di cui 7 in servizio) (cfr. sez. IV, tab. 17, 18).

Particolare attenzione è stata riservata, anche nel 2015, all'artività formariva per il personale. In particolare, la convenzione stipulata con la Sna ha consentito la partecipazione di un elevato numero di dipendenti ai corsi di formazione da questa organizzati. Tra i corsi maggiormente seguiti dal personale dell'Autorità si possono citare in particolare quelli relativi ai processi di comunicazione nella p.a.. Sono stati tenuti, inoltre, da varie unità organizzative dell'Ufficio, diversi seminari formativi interni, su temi di particolare interesse per l'attività del Garante. A titolo di esempio si citano i seminari sulla riforma della normativa europea sulla protezione dei dati personali, nonché i corsi di aggiornamento sugli applicativi più comunemente usati per una migliore gestione dei documenti informatici.

L'Autorità ha inoltre erogato dei corsi di formazione di lingua inglese prevalentemente mirati al personale impegnato nelle attività comunitarie ed internazionali.

Complessivamente, nel corso dell'anno sono state somministrate circa 460 ore di formazione, usufruite da oltre metà del personale.

L'Autorità ha continuato ad avvalersi delle figure professionali previste dalla vigente normativa in materia di sicurezza e incolumità dei lavoratori nei luoghi di lavoro (medico competente e responsabile del servizi di prevenzione e sicurezza), i cui contratti, tuttavia, sono stati prorogati solo per il tempo necessario a verificare le condizioni della convenzione Consip in materia. Presso l'Autorità opera il servizio di controllo interno che è presieduto da un magistrato della Corte dei conti e composto da due dirigenti generali, rispettivamente, della Ragioneria generale dello Stato e della Presidenza del Consiglio dei ministri.

25.5. *Il settore informatico e tecnologico*

Sviluppo del sistema informativo e dei servizi ICT

Nel 2015 è proseguita l'attività di sviluppo del sistema informativo nel solco delle direttrici di innovazione tracciate dal Cad, con enfasi sulla smaterializzazione dei flussi documentali e sulla cooperazione interna. Sono stati analizzati nuovi flussi documentali inerenti l'attività dell'organo collegiale, con la gestione dei provvedimenti, dell'ordine del giorno delle adunanze e delle deliberazioni del Garante. I nuovi flussi consentono di tracciare l'*iter* di approvazione a partire dagli schemi di provvedimento presentati dalle diverse unità dell'Ufficio. Le procedure sono state implementate sulla piattaforma di *test* per svolgere un periodo di prova preliminare alla messa in produzione nel mese di aprile 2016. È stata inoltre introdotta una nuova procedura *client server* di gestione del bilancio in ambiente Microsoft Windows in sostituzione del prodotto utilizzato, a partire dal 2002, in ambiente Unix Solaris. Dal punto di vista infrastrutturale, è proseguita l'azione di consolidamento delle architetture a supporto dell'applicazione del sistema informativo, con l'acquisizione di nuovi sistemi di *storage* e nuovi apparati di *switching* Fiber Channel, nonché la ristrutturazione della piattaforma di virtualizzazione.

Sicurezza informatica dell'Ufficio

Nel 2015 nessun evento relativo alla sicurezza ha prodotto danni o disservizi nel dominio dell'Ufficio. Si sono registrati casi sporadici dovuti all'azione di *malware* di tipo *cryptolocker* su postazioni individuali, cui si è posto rimedio grazie alle ordinarie procedure di *backup* e *recovery* e con l'intensificazione delle azioni informative atte a prevenire i rischi. La continuità dei servizi accessibili al pubblico (notificazione dei trattamenti) è stata conforme, dal punto di vista quantitativo, a quella del 2014, con valori di *downtime* inferiori alle otto ore complessive nell'arco dell'anno e solo per interventi straordinari a seguito di guasti *hardware*.

Attività di consulenza e cooperazione interna ed esterne

Il Dipartimento ha collaborato con le altre unità organizzative dell'Ufficio nella trattazione di procedimenti e attività ispettive, in particolare nei casi di:

- trattamenti di profilazione con finalità di *marketing* definendo le misure tecnico-organizzative volte al rispetto del principio di minimizzazione dei dati, anche mediante una opportuna separazione fisica e logica dei sistemi preposti allo scopo e alla precisa allocazione di responsabilità nell'ambito dei processi aziendali (cfr. par 11.1);
- *data breach*, sia in ambito pubblico che privato, in riferimento all'utilizzo di moderne tecnologie per garantire la sicurezza o per consentire il monitoraggio del servizio pubblico locale atttaverso apparecchi per videosorveglianza e di scatole nere (*black box*) installate sugli autoveicoli dotate, tra l'altro, di funzionalirà di geolocalizzazione (cfr. par. 11.7);
- trattamenti di dati biometrici (cfr. cap. 14);
- trattamento di dati sanitari (cfr. cap. 5);
- *Internet of Things* (cfr. par. 10.3);
- attività internazionali del Garante, in particolare nell'ambito del sottogruppo *Technology* del Gruppo Art. 29 e il Gruppo di Berlino (cfr. par. 22.5).

PAGINA BIANCA

I dati statistici

PAGINA BIANCA

IV - I dati statistici 2015

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	692
Pareri a Presidenza del Consiglio dei ministri e ministeri (art. 154, comma 4, del Codice)	44
Autorizzazioni individuali al trattamento dei dati sensibili e giudiziari (art. 41 del Codice)	1
Provvedimenti concernenti trasferimenti di dati consentiti verso Paesi terzi (art. 44, comma 1, lett. *a*), del Codice)	5
Decisioni su ricorso (art. 145 del Codice)	307
Provvedimenti collegiali su segnalazioni e reclami (artt. 142-144), a seguito di accertamenti d'ufficio (art. 154), nonché artt. 13, comma 5, lett. *c*), 150, comma 5, del Codice	57
Ordinanze-ingiunzione adottate dal Garante	206
Riscontri a segnalazioni, reclami, richieste di parere e quesiti (artt. 142-144 del Codice e artt. 5 e 11, Reg. Garante n. 1/2007)	4.991
Provvedimenti collegiali su verifiche preliminari per trattamenti che presentano rischi specifici (art. 17 del Codice)	27
Comunicazioni al Garante su flussi di dati tra p.a. o in materia di ricerca scientifica (artt. 19, comma 2, 39 e 110 del Codice)	12
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari (art. 154, comma 1, lett. *g*)	12
Risposte ad atti di sindacato ispettivo e di controllo	7
Risposte a quesiti	25.528
Rilievi formulati in relazione a leggi regionali ai fini dell'impugnazione *ex* art. 127 Cost.	2
Accertamenti e controlli effettuati *in loco* (artt. 157-158 del Codice)	303
Violazioni amministrative contestate	1.696
Sanzioni applicate con ordinanza di ingiunzione	294
Pagamenti derivanti dall'attività sanzionatoria	€ 3.345.515
Comunicazioni di notizia di reato all'autorità giudiziaria	33
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	14
Ricorsi (trattati) *ex* art. 152 del Codice	19
Opposizioni (trattate) a provvedimenti del Garante	85
Notificazioni pervenute nell'anno 2015	2.622
Notificazioni pervenute dal 2004 al 31 dicembre 2015	26.691
Riunioni del Gruppo Art. 29	6
Partecipazione a sottogruppi di lavoro - Gruppo Art. 29	36
Riunioni autorità comuni di controllo (Europol, SIS II, Dogane, Eurodac, VIS)	23
Conferenze internazionali	2
Riunioni presso il CoE, OCSE e altri organismi internazionali	8
Riunioni e *workshop* presso Consiglio/Commissione e altri organismi UE	26
Quesiti, questionari e richieste di contributi provenienti da altre Autorità e Istituzioni	28

Tabella 1. Sintesi delle principali attività dell'Autorità

Attività di comunicazione dell'Autorità	
Comunicati stampa	34
Newsletter	13
Prodotti editoriali	2
Prodotti web	9

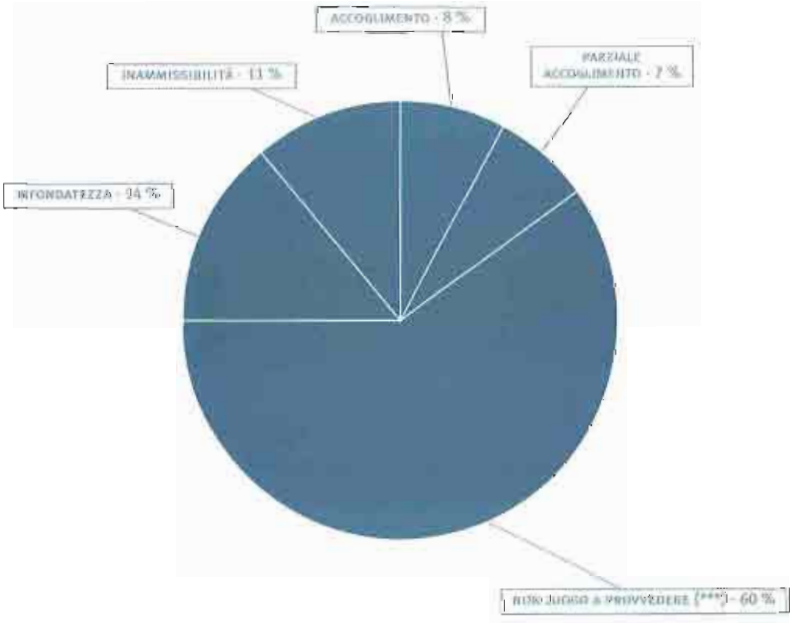
Tabella 2. Attività di comunicazione dell'Autorità

Tabella 3. Pareri *ex* art. 154, comma 4, del Codice

Pareri *ex* art. 154, comma 4, del Codice	
Temi	Riscontri resi nell'anno (*)
Informatizzazione e banche dati della p.a.	15
Attività di polizia, sicurezza nazionale e governo del territorio	8
Dati sanitari	8
Fisco e valuta	5
Processo telematico	4
Formazione	4
Totale	44

Tabella 4. Tipologia delle decisioni su ricorsi

Decisioni su ricorsi	
Tipi di decisione (**)	Numero ricorsi
Accoglimento	23
Parziale accoglimento	23
Non luogo a provvedere (***)	183
Infondatezza	44
Inammissibilità	34
Totale	307



(*) Inerenti anche ad affari pervenuti anteriormente al 2015

(**) Le decisioni sui ricorsi possono contenere più statuizioni in base alle diverse richieste presentate: la statistica prende in esame, in tali casi, la statuizione più "favorevole" al ricorrente

(***) Casi nei quali le richieste del ricorrente sono state soddisfatte nel corso del procedimento

Categorie di titolari	Numero ricorsi
Banche e società finanziarie	73
Compagnie di assicurazione	10
Sistemi di informazioni creditizie	13
Società di informazioni commerciali	23
Amministrazioni pubbliche e concessionari di pubblici servizi	20
Strutture sanitarie pubbliche e private	7
Parrocchie	1
Fornitori telefonici e telematici	19
Attività di *marketing* svolta da imprenditori privati	17
Datori di lavoro pubblici e privati	22
Editori (anche televisivi)	74
Liberi professionisti	3
Amministrazioni condominiali	4
Altri	21
Totale	307

Tabella 5. Suddivisione dei ricorsi in relazione alle categorie di titolari del trattamento

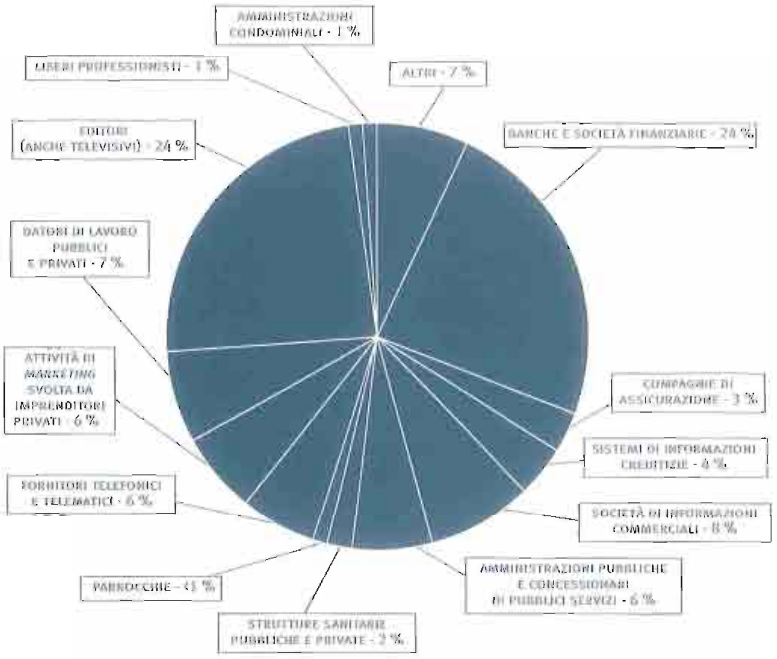
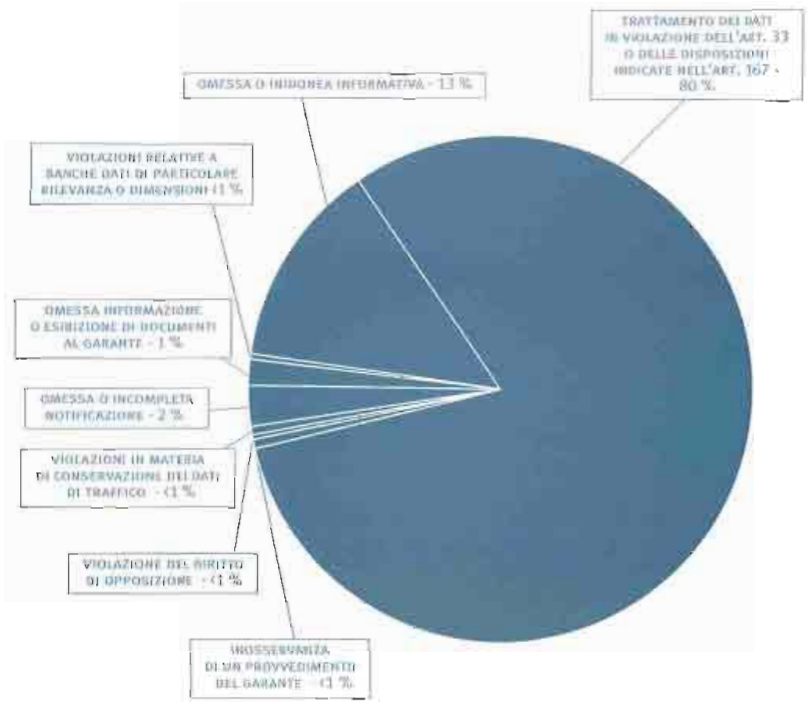


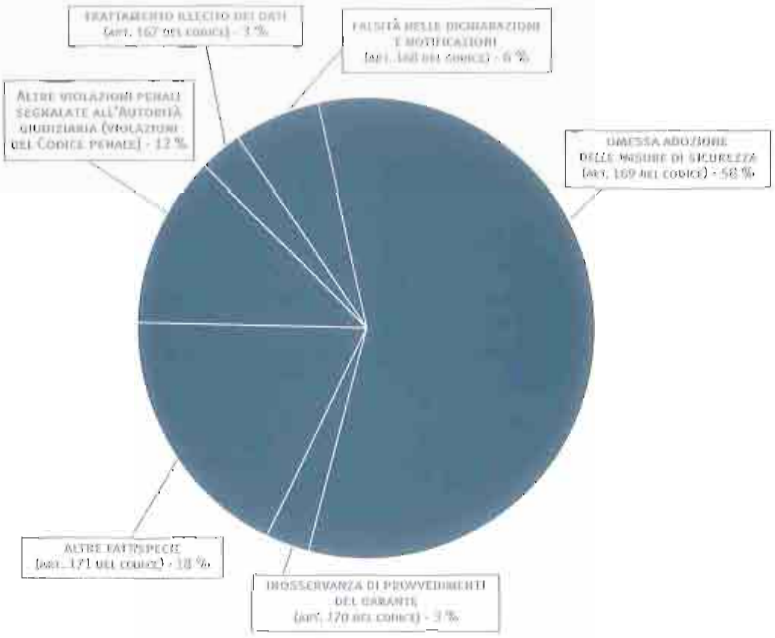
Tabella 6. Violazioni amministrative contestate

Violazioni amministrative contestate	
Omessa o inidonea informativa (art. 161 del Codice)	223
Trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis*, del Codice)	1371
Inosservanza di un provvedimento del Garante (art. 162, comma 2-*ter*, del Codice)	10
Violazione del diritto di opposizione (art. 162, comma 2-*quater*, del Codice)	5
Violazioni in materia di conservazione dei dati di traffico (art. 162-*bis* del Codice)	9
Omessa o incompleta notificazione (art. 163 del Codice)	44
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)	28
Violazioni relative a banche dati di particolare rilevanza o dimensioni (art. 164-*bis*, comma 2, del Codice)	6
Totale	1696



Comunicazioni di notizia di reato all'autorità giudiziaria	
	Segnalazioni
Trattamento illecito dei dati (art. 167 del Codice)	1
Falsità nelle dichiarazioni e notificazioni (art. 168 del Codice)	2
Omessa adozione delle misure di sicurezza (art. 169 del Codice)	19
Inosservanza di provvedimenti del Garante (art. 170 del Codice)	1
Altre fattispecie (art. 171 del Codice)	6
Altre violazioni penali segnalate all'Autorità giudiziaria (violazioni del codice penale)	4
Totale	33

Tabella 7. Comunicazioni di notizia di reato all'autorità giudiziaria



Pagamenti derivanti dall'attività sanzionatoria	
Somme versate a titolo di oblazione in via breve	1.647.468
Somme versate in conseguenza di ordinanze ingiunzione	1.170.930
"Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169 del Codice)"	270.000
Ulteriori entrate derivanti dall'attività sanzionatoria	257.117
Totale	3.345.515

Tabella 8. Pagamenti derivanti dall'attività sanzionatoria

Quesiti		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale quesiti	259	353

Tabella 9. Quesiti

(*) Inerenti anche ad affari pervenuti anteriormente al 2015

Tabella 10. Segnalazioni e reclami

Segnalazioni e reclami		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale segnalazioni e reclami	3.650	4.638
Temi principali		
Assicurazioni	44	26
Associazioni	40	36
Centrali rischi	108	100
Concessionari pubblici servizi	57	30
Condominio	24	31
Credito	261	266
Data breach	33	32
Enti locali	108	108
Giornalismo e libertà d'espressione	205	290
Imprese	121	107
Informazioni commerciali	4	15
Internet	175	238
Istruzione	62	62
Lavoro	201	51
Marketing (posta cartacea, *e-mail*, fax, sms)	307	441
Marketing telefonico	1.412	1.695
Recupero crediti	93	78
Sanità e servizi di assistenza sociale	101	101
Videosorveglianza	234	150

Tabella 11. Atti di sindacato ispettivo e controllo

Atti di sindacato ispettivo e controllo	
Temi	Numero
Esercizio dei diritti fondamentali	3
Trattamento di dati personali nell'attività di promozione commerciale svolta mediante *call center*	2
Cyberbullismo	1
Centrali rischi	1
Totale	7

Tabella 12. Tipologie di notificazioni pervenute nel periodo 2004-2015

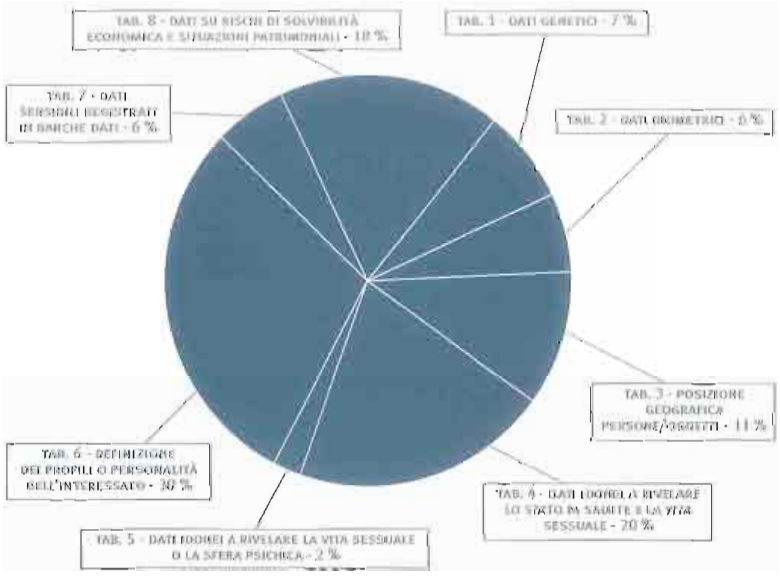
Tipologie di notificazioni pervenute nel periodo 2004-2015 (**)			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute (**)
Prima notificazione al Garante	1.256	19.820	21.076
Modifica di una precedente notificazione	180	4.292	4.472
Notificazione della cessazione del trattamento	89	1.054	1.143
Totale	1.525	25.166	26.691

(*) Inerenti anche ad affari pervenuti anteriormente al 2015

(**) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2015

Suddivisione delle notificazioni per tipologia di trattamento svolto 2004-2015	
Tabelle di notificazione compilate (*)	Numero
Tabella 1 - Trattamento di dati genetici	2.875
Tabella 2 - Trattamento di dati biometrici	2.425
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	4.186
Tabella 4 - Trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria	8.085
Tabella 5 - Trattamento di dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale	871
Tabella 6 - Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con l'esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi	11.669
Tabella 7 - Trattamento di dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie	2.280
Tabella 8 - Trattamento di dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti	7.014
Totale (**)	39.405

Tabella 13. Suddivisione delle notificazioni per tipologia di trattamento effettuato: 2004-2015



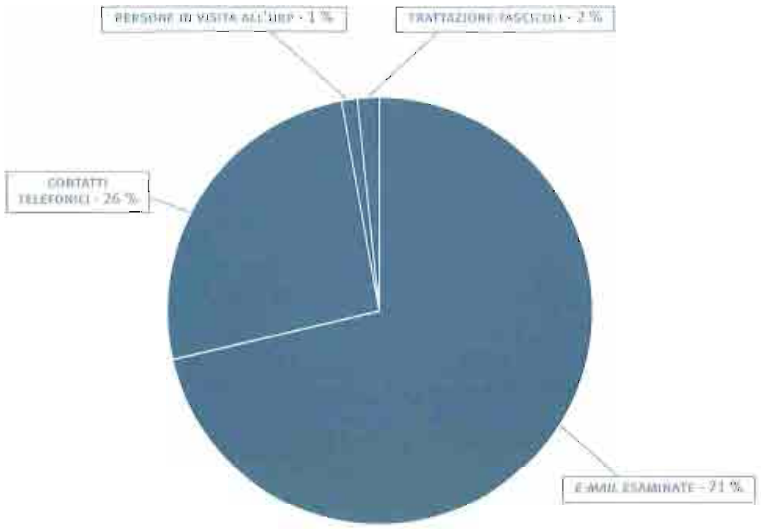
(*) Situazione alla data del 31 dicembre 2015
(**) N.B. Il totale è superiore alla sommatoria delle precedenti tabelle in quanto una singola notificazione può riguardare più trattamenti

Tabella 14. Tipologie di notificazioni pervenute nel 2015

Tipologie di notificazioni pervenute nel 2015 (*)			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute (*)
Prima notificazione al Garante	46	1.661	1.707
Modifica di una precedente notificazione	27	744	771
Notificazione della cessazione del trattamento	16	128	144
Totale	89	2.533	2.622

Tabella 15. Ufficio relazioni con il pubblico

Ufficio relazioni con il pubblico	
	2015
E-mail esaminate	18.214
Contatti telefonici	6.572
Persone in visita all'Urp	310
Trattazione fascicoli	432
Totale	25.528



(*) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2015

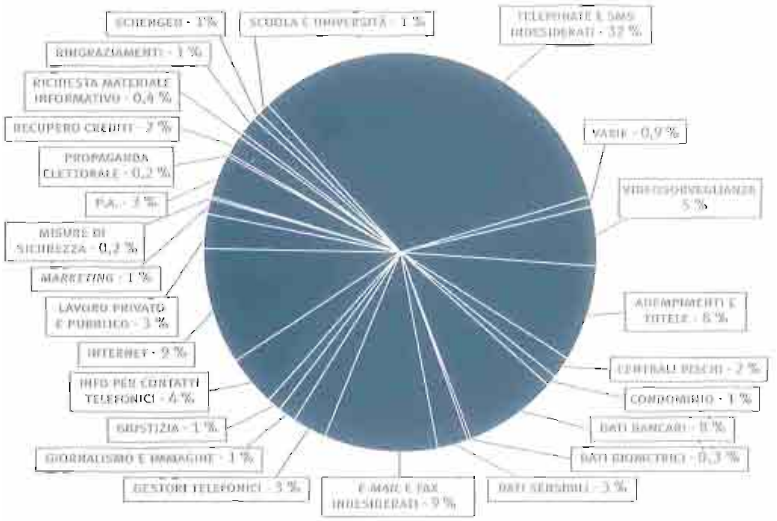


Grafico 16. *E-mail* esaminate dall'Ufficio relazioni con il pubblico

Posti previsti in organico	
Segretario generale	1
Dirigenti	21
Funzionari	88
Operativi	26
Esecutivi	1
Totale	137
Personale a contratto	8

Tabella 17. Posti previsti in organico

Tabella 18. Personale in servizio

Personale in servizio (*)				
Area	In ruolo (a)	In posizione di fuori ruolo (b)	Comandato presso altre amministrazioni o in aspettativa (c)	Impiegato dall'Ufficio (a+b-c)
Segretario generale	1	–	–	1
Dirigenti	13	2		15
Funzionari	71	2	2	71
Operativi	24			24
Esecutivi	–	–	–	–
Totali	109	4	2	111
Personale a contratto				7

Tabella 19. Risorse finanziarie

Risorse finanziarie						
Entrate accertate	Anno 2015		Anno 2014		Differenza	
Entrate correnti		19.241.951		20.969.494		-8,24%
di cui trasferimento dallo Stato	6.875.993		7.621.271		-9,78%	
Totale entrate		19.241.951		20.969.494		-8,24%
Spese impegnate	Anno 2015		Anno 2014		Differenza	
Spese di funzionamento		18.045.363		18.048.088		-0,02%
Spese in conto capitale		414.296		374.020		10,77%
Rimborsi al Mef e transazioni		253.612		673.612		-62,35%
Totale spese		18.713.271		19.095.720		-2,00%

(*) Situazione alla data del 31 dicembre 2015

Tabella 20. Attività internazionali dell'Autorità

Unione europea		
Gruppo Articolo 29	Sessione plenaria Art. 29	3 e 4 febbraio 14 e 15 aprile 16 e 17 giugno 22 e 23 settembre 15 ottobre 16 dicembre
	Riunioni dei sottogruppi — *Border Travel Law Enforcement* (BTLE)	12 gennaio 24 marzo 21 maggio 30 luglio (gruppo di lavoro) 3 settembre 3 novembre
	Riunioni dei sottogruppi — *Cooperation*	29 maggio 22 luglio 6 novembre 17 e 18 novembre (*workshop*)
	Riunioni dei sottogruppi — *E-Government*	20 marzo 5 maggio 1 settembre 5 novembre
	Riunioni dei sottogruppi — *Financial Matters*	17 febbraio 20 aprile 4 settembre 21 ottobre
	Riunioni dei sottogruppi — *Future of Privacy*	20 gennaio 11 marzo 22 maggio 8 giugno (gruppo di lavoro) 22 luglio 7 settembre 6 novembre
	Riunioni dei sottogruppi — *Key Provision*	26 marzo 12 maggio
	Riunioni dei sottogruppi — *International Transfers*	8 gennaio 19 marzo 21 maggio 8 ottobre
	Riunioni dei sottogruppi — *Technology*	13 e 14 gennaio 3 e 4 marzo 19 e 20 maggio 9 settembre 3 e 4 novembre

Unione europea	
Autorità di controllo comune EUROPOL	8 gennaio (incontro al Parlamento europeo) 19-22 gennaio (attività ispettiva) 4 marzo 9-13 marzo (attività ispettiva) 3 giugno 22 giugno (incontro al Parlamento europeo) 16 luglio (Sottogruppo NPG) 10 e 11 settembre (Sottogruppo NPG) 12 ottobre 10 dicembre
Autorità di controllo comune DOGANE	4 giugno 11 dicembre
Gruppo di coordinamento della supervisione SID	4 giugno 11 dicembre
Gruppo di coordinamento della supervisione SIS II	17-18 febbraio (*workshop*) 25 marzo 9 giugno 22 settembre (*technical expert group*) 7 ottobre
Gruppo di coordinamento della supervisione EURODAC	6 marzo 8 ottobre
Gruppo di coordinamento della supervisione VIS	26 marzo 8 ottobre

Unione europea		
Riunioni di gruppi di esperti	Consiglio UE - Dapix (Regolamento)	15 e 16 gennaio 5-6 febbraio 23-24 marzo 30-31 marzo 21 e 22 aprile 6 e 7 maggio 18 e 19 maggio 22 luglio 2 settembre
	Consiglio UE - Dapix (Direttiva)	20 aprile 15-16 luglio 4 settembre 9 setrembre 16 settembre 21-22 settembre 30 ottobre 6 novembre 13 novembre 19- 20 novembre 26 novembre 1-2 dicembre
Commissione UE – *Meeting* con esperti nazionali PNR		13 gennaio 17 marzo
Comitato *ex* Art. 31 direttiva 95/46/CE		14 gennaio 16 luglio
Commissione UE - *Data breach notifications under the e-Privacy Directive*		6 ottobre

Altri *forum* internazionali		
Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	Comitato "*Working Party on Security and Privacy in the Digital Economy* "	10 aprile (*conference call*) 13 maggio (*conference call*) 12 giugno (*conference call*) 22 giugno 21 ottobre (ADG *task force*) 5 novembre (*conference call*) 17 novembre (*conference call*) 30 novembre (ADG *task force*) 1 dicembre
	Plenaria	23-24 giugno 1-2 dicembre
Consiglio d'Europa	Comitato T-PD *Bureau*	25-27 marzo 6-8 ottobre
Gruppi di lavoro specifici	Gruppo internazionale di lavoro sulla protezione dei dati nelle telecomunicazioni (IWGDPT)	27 e 28 aprile 13-14 ottobre
International Enforcement	IECWG (*International Enforcement Coordination Working Group*)	11 luglio (*conference call*)
	Progetto PHAEDRA	27 ottobre (*workshop*) 25 novembre (*workshop*)
	GPEN (*Global Privacy Enforcement Network – Sweep*)	27 gennaio (*conference call*) 21 aprile (*conference call*) 21 luglio (*conference call*)

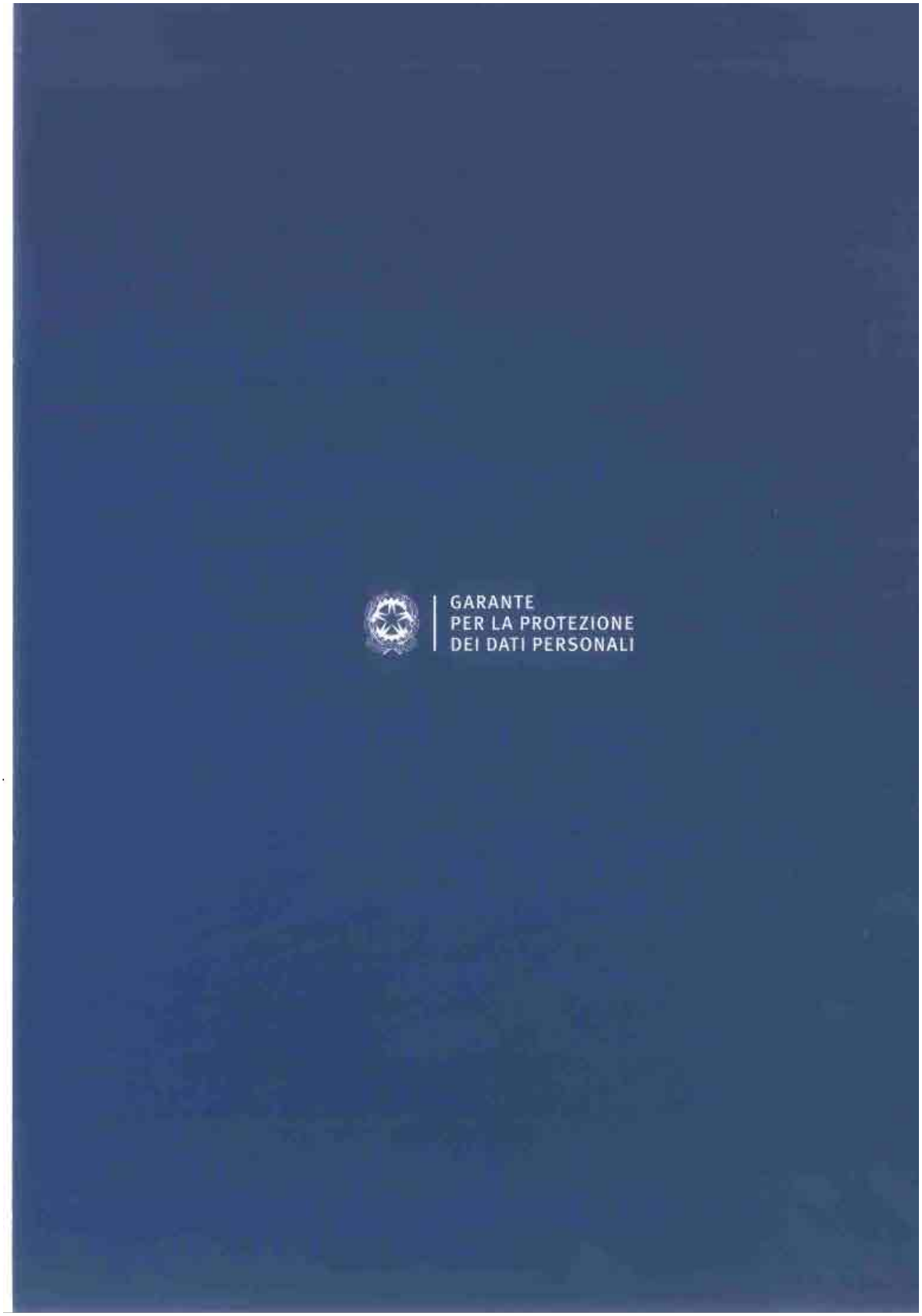
Conferenze internazionali	
Conferenza di primavera delle Autorità europee di protezione dati	18-20 maggio, Manchester
37ª Conferenza internazionale delle Autorità di protezione dati	26-29 ottobre, Amsterdam

Altre conferenze e *meeting*	
JHA *Taiex Workshop*	31 marzo, Podgorica
CPDP *Conference "Data Protection on the Move"*	21-23 gennaio, Bruxelles
International Conference on the Privacy and Data Protection Implications of the Civil Use of Drones	5 e 6 febbraio, Budapest
Workshop Big Data – The Accountability Foundation	29 aprile, Madrid 14 luglio, Roma
3rd *Workshop pan-European Personal Data Breach Exercise*	23-24 giugno, Ispra
Annual Privacy Forum – Enisa	7 e 8 ottobre, Lussemburgo
Trust, privacy and security conference	17, 19 novembre, Sofia
Workshop "The grey areas between media regulation and data protection"	11 dicembre, Strasburgo
Meeting on the Health privacy Code of Conduct	7 dicembre, Bruxelles

Redazione
Garante per la protezione dei dati personali

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 696773785
e-mail: garante@gpdp.it
www.garanteprivacy.it

stampa:
UGO QUINTILY S.p.A.


GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

PAGINA BIANCA

171360015340