GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione2017

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771
email: garante@gpdp.it
www.garanteprivacy.it

Relazione2017

www.garanteprivacy.it

I numeri del 2017

Provvedimenti collegiali 573

276
Ricorsi decisi

116
Ordinanze-ingiunzione

26
Verifiche preliminari

19
Pareri resi al Governo

38
Pareri accesso civico

5.819
Riscontri a segnalazioni e reclami

€ 3.776.694
Sanzioni riscosse

275
Ispezioni

589
Sanzioni contestate

3.179
Notificazioni pervenute

41
Comunicazioni all'autorità giudiziaria

16.193
Risposte a quesiti

54
Comunicati e *newsletter*

5.202.264
Accessi al sito web

In evidenza – 2017

Gennaio

Siamo nuovamente intervenuti nel settore delle telefonate commerciali indesiderate, vietando ad una società di servizi informatici l'utilizzo delle utenze telefoniche reperite in internet – in genere ricercando i numeri di telefono di liberi professionisti e di imprese individuali presenti nell'area "contatti" dei siti web visionati –, ponendosi tale trattamento in violazione del principio di finalità, oltre ad essere effettuato senza il consenso informato degli interessati. I contatti presenti in rete, infatti, ancorché liberamente conoscibili, non sono per ciò solo utilizzabili per qualsiasi finalità, essendo, nel caso considerato, preordinati ad agevolare l'attività professionale dei soggetti cui si riferiscono [par. 10.3]

Abbiamo autorizzato, in ragione dell'attività svolta, il trattamento di dati giudiziari, con particolare riferimento a quelli inerenti i delitti contro il patrimonio e la personalità interna dello Stato, riferiti a specifiche figure professionali di una società che opera anche nell'interesse di soggetti istituzionali in settori altamente strategici per il Paese [par. 13.6]

Nel corso dell'intero anno si sono susseguite numerose attività ispettive, sul territorio nazionale e al di fuori di esso, cooperando con l'Autorità di controllo albanese, per contrastare il fenomeno del cd. *telemarketing* selvaggio, in particolare svolto nell'interesse di operatori telefonici ed energetici: numerosi provvedimenti con i quali sono stati accertati (e in parte già sanzionati) milioni di contatti illeciti ed impartite articolate prescrizioni sono stati adottati nel 2017 (e nei primi mesi del 2018) [parr. 10.2 e 10.3]

Febbraio

A partire da febbraio, con una pluralità di pareri resi a responsabili della prevenzione e della corruzione o a difensori civici ai sensi dell'art. 5, commi 7 e 8, d.lgs. n. 33/2013, ci siamo pronunciati sulle variegate fattispecie sottoposte al Garante, orientando le decisioni delle amministrazioni richiedenti in ordine all'accoglimento o meno (in base a quanto previsto dall'art. 5, comma 2-*bis*, lett. *a*), d.lgs. n. 33/2013), dell'accesso civico in presenza di un pregiudizio concreto alla protezione dei dati personali [par. 4.3.1]

Abbiamo reso al Ministero dell'interno un articolato parere sullo schema di decreto – destinato ad essere pubblicato nella Gazzetta Ufficiale ed inserito come allegato al Codice (Allegato C) – con il quale sono stati individuati, in conformità a quanto stabilito dall'art. 53, comma 2, del Codice, i trattamenti non occasionali di dati personali effettuati con strumenti elettronici presso il Ced del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici nell'esercizio delle attribuzioni conferite da disposizioni di legge o di regolamento per finalità di polizia [par. 7.3]

Nell'ambito di un'indagine della Procura della Repubblica di Roma, limitatamente alle riscontrate violazioni di natura amministrativa, abbiamo comminato sanzioni per oltre 11 milioni di euro a cinque società che operano nel settore del *money transfer* per aver trattato in modo illecito dati personali di oltre mille persone inconsapevoli. I dati personali degli (ignari) interessati venivano illecitamente utilizzati per trasferire in Cina, con la tecnica del frazionamento, somme di denaro in realtà riconducibili a imprenditori cinesi [par. 21.5.2]

Marzo

Abbiamo reso parere su uno schema di decreto del Presidente della Repubblica, adottato ai sensi dell'art. 57 del Codice, nel quale – già recependo molte delle richieste avanzate dall'Autorità in fase istruttoria – vengono fissate le modalità di attuazione dei principi del Codice rispetto ai tratta-

menti di dati effettuati dalle Forze di polizia nell'attività di prevenzione e repressione dei reati, di tutela dell'ordine e della sicurezza pubblica. Nell'esprimere il parere, abbiamo richiesto al Ministero di integrare il testo al fine di sottoporre alle regole di protezione dei dati i trattamenti che presentano rischi specifici per la persona (banche di dati genetici, biometrici, dati relativi all'ubicazione, banche dati basate su particolari tecniche di elaborazione delle informazioni, ecc.) e di stabilire tempi di conservazione più brevi, commisurati alle finalità della raccolta, rispetto a quelli in essere [par. 7.3]

Nell'ambito di una verifica preliminare richiesta da una società che eroga servizi idrici e concernente il trattamento della posizione dei propri automezzi per una molteplicità di finalità, rilevato che dal sistema di geolocalizzazione poteva derivare un controllo a distanza dei lavoratori, abbiamo ritenuto che, anche dopo le modifiche introdotte dal cd. *Jobs Act*, fosse necessario un apposito accordo con le rappresentanze sindacali o, in sua assenza, l'autorizzazione dell'Ispettorato nazionale del lavoro. Abbiamo inoltre richiesto alla società istante, oltre che di fornire un'informativa completa ai dipendenti, di definire le modalità di raccolta, di elaborazione e di conservazione dei dati di geolocalizzazione e degli altri dati personali, differenziando le tutele in base alla singola finalità perseguita. Abbiamo inoltre ritenuto di escludere il monitoraggio dei tracciati percorsi, salvo il possibile trattamento dei relativi dati in forma aggregata o anonima per finalità statistiche e di programmazione del lavoro [par. 13.2]

Nel rendere il parere sullo schema dell'ultimo decreto interministeriale attuativo del funzionamento della banca dati del Dna – concernente le modalità di cancellazione, immissione, distruzione e conservazione dei profili di Dna – abbiamo richiesto che le informazioni genetiche e gli altri dati personali contenuti nella banca dati siano costantemente aggiornati, anche alla luce delle comunicazioni processuali, e non in base a intervalli predeterminati, così da assicurare la correttezza del trattamento (in particolare, con la tempestiva cancellazione dei dati riferibili a chi è stato assolto con sentenza definitiva perché il fatto non sussiste, perché l'imputato non lo ha commesso, perché il fatto non costituisce reato o perché il fatto non è previsto dalla legge come reato). Abbiamo anche segnalato l'importanza di fornire un'adeguata informativa alle persone i cui profili sono registrati in banca dati, la necessità di chiarire le regole che impongono la cancellazione di un profilo di Dna nonché di individuare con maggiore precisione quali siano i soggetti nazionali che hanno il diritto di accedere a dati così delicati [par. 7.4]

Abbiamo reso parere favorevole allo schema di regolamento che disciplina le modalità di funzionamento del Registro tumori della Regione Lazio che individua le tipologie di dati sensibili, le operazioni eseguibili e le specifiche finalità perseguite dal Registro nonché i soggetti che possono avervi accesso e le misure per la custodia e la sicurezza dei dati. Lo schema, che ha accolto in fase di predisposizione gran parte delle nostre indicazioni, mirate a garantire elevati standard di sicurezza nel trattamento dei dati, la corretta indicazione delle finalità nonché il rispetto dei principi di essenzialità e indispensabilità, necessita di alcuni ulteriori accorgimenti specie sotto il profilo della delimitazione delle operazioni di trattamento a quelle realmente necessarie e delle misure di sicurezza [par. 6.1]

Aprile

In materia di *data breach*, a seguito di approfondite verifiche effettuate a partire dal dettagliato reclamo di un utente relativo all'ingiustificata attivazione a suo nome e a propria insaputa di un numero elevato di linee di telefonia residenziale (oltre 800) da parte di uno dei principali gestori di telefonia, abbiamo appurato che tale erronea attribuzione sarebbe derivata da errori occorsi durante le attività di migrazione massiva dei dati della clientela dal sistema gestionale preesistente a quello in uso e ha inte-

ressato, per un lungo arco temporale, un ampio novero di soggetti. Nello stigmatizzare la condotta negligente e omissiva tenuta dal titolare del trattamento – il quale, durante un prolungato arco temporale, anche in tempi successivi alla segnalazione dell'erroneità delle assegnazioni delle utenze, in violazione del principio di correttezza nel trattamento, non ha svolto le necessarie verifiche, che avrebbero potuto assicurare l'approntamento di rimedi nei confronti del reclamante anzitutto e, quindi, di quanti si trovano in una situazione analoga –, abbiamo impartito analitiche prescrizioni nei confronti dello stesso, monitorandone costantemente l'attuazione, e provveduto a contestare le sanzioni amministrative per le violazioni rilevate [par. 11.3]

Abbiamo respinto la richiesta di una società, specializzata nella riparazione e sostituzione di cristalli per autoveicoli, di adottare un provvedimento di bilanciamento di interesse al fine di costituire una banca dati preordinata alla raccolta di informazioni utili a verificare eventuali condotte fraudolente in campo assicurativo senza richiedere il consenso degli interessati. Le attività di prevenzione e contrasto di fenomeni fraudolenti sono infatti disciplinate per via legislativa con l'attribuzione della gestione delle banche di dati a tal fine istituite in capo a soggetti pubblici muniti di idonee garanzie di terzietà, diversamente dalla società richiedente [par. 14.2.2]

Maggio

Abbiamo ritenuto illecito il trattamento dei dati effettuato in occasione del rinnovo/rilascio della Carta multiservizi della difesa e prescritto un programma di aggiornamento delle Cmd volto ad inibire il trattamento dei dati biometrici memorizzati in violazione delle disposizioni vigenti. È stato sottolineato che esclusivamente in caso di trattamenti effettuati per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge che li prevedano specificamente, alcuni articoli del Codice non trovano applicazione. In tutti gli altri casi il trattamento di dati relativi alle impronte digitali è ammesso a condizione che sia sottoposto, con esito positivo, a verifica preliminare [par. 13.5]

Senza soluzione di continuità, a partire da maggio abbiamo intrapreso un'azione di ascolto e comunicazione, con il settore pubblico e privato, in vista dell'applicazione, a far data dal 25 maggio 2018, del Regolamento generale sulla protezione dei dati personali (RGPD) [parr. 1.10, 1.11 e 23.1]

Giugno

Abbiamo rigettato l'istanza di una società che chiedeva di essere autorizzata ad effettuare un trattamento di dati giudiziari dei propri dipendenti mediante la raccolta ed il successivo trattamento del certificato tratto dal casellario giudiziale al fine di soddisfare una clausola contrattuale di appalto che prevedeva la comunicazione degli esiti nonché la tempestiva segnalazione al committente dei lavoratori impiegati a carico dei quali risultavano sentenze di condanna passate in giudicato nonché dei reati ascritti e della pena comminata. Abbiamo quindi ribadito che il trattamento dei dati giudiziari da parte del datore di lavoro può essere effettuato solo in presenza di un'idonea base giuridica (legislativa, regolamentare o contrattuale) [par. 13.6]

A seguito di segnalazioni e verifiche *in loco*, abbiamo dichiarato illecito l'utilizzo di una consistente banca dati impiegata per l'attività di *telemarketing* nel settore odontoiatrico, acquisita dal titolare del trattamento da un fornitore di liste stabilito al di fuori del territorio nazionale [par. 10.3]

Luglio

Abbiamo espresso i pareri richiesti in materia di anticipo finanziario a garanzia pensionistica (Ape), dapprima fornendo indicazioni sul contenuto dell'informativa da fornire agli interessati, sui ruoli assunti nel tratta-

mento dei dati e sulle misure necessarie ad assicurare la minimizzazione dei dati nella trasmissione dei messaggi di posta elettronica; quindi, pronunciandoci sugli schemi dell'Accordo quadro per l'Ape e sull'Accordo quadro per la polizza assicurativa obbligatoria per il rischio di premorienza da stipularsi tra il Ministro dell'economia e delle finanze e il Ministro del lavoro e delle politiche sociali, l'Associazione bancaria italiana e l'Associazione nazionale fra le imprese assicuratrici [par. 4.8]

Abbiamo reso parere favorevole allo schema di d.P.R. relativo alle procedure di raccolta, accesso, comunicazione, cancellazione e integrazione dei dati registrati nel Ced che conclude, unitamente ai pareri resi a febbraio e marzo, l'*iter* di regolamentazione dei dati personali trattati a fini di polizia, dando così completa attuazione al Titolo II della parte II del Codice. Lo schema presentato ha tenuto conto delle indicazione fornite dall'Ufficio nel corso di più riunioni volte a perfezionare il testo e renderlo conforme alla disciplina di protezione dati. È stata infatti introdotta la figura del Responsabile protezione dati cui sono affidati i compiti di informazione e vigilanza, disciplinata l'organizzazione del Ced e sono state stabilite le regole di conservazione e comunicazione dei dati. Abbiamo rilevato l'opportunità di dettagliare con atto di natura regolamentare le misure di sicurezza specifiche nonché di precludere l'estrazione e la copia in forma massiva delle informazioni confluite nel Ced [par. 7.3]

Nei tempi previsi dalla legge 29 maggio 2017, n. 71, a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo, abbiamo dato riscontro a tutte le segnalazioni pervenute (concernenti la creazione di falsi profili, talvolta finalizzati allo scambio di messaggi a sfondo sessuale, diffusione di messaggi offensivi e denigratori e/o di fotografie scattate in ambito privato), attivandoci a tutela degli interessati presso i gestori di *social media* e di siti web localizzati in ambito europeo ed extraeuropeo [cap. 9]

Settembre

Al fine di favorire il rispetto degli obblighi vaccinali nei tempi ristretti previsti dal legislatore, abbiamo autorizzato, con procedura d'urgenza (in considerazione dell'imminente avvio dell'anno scolastico), la comunicazione dei dati personali non sensibili dalle scuole alle autorità sanitarie, per consentire un trattamento dei dati non previsto dalla normativa sui vaccini se non a partire dal 2019 [par. 5.2.1]

Abbiamo riscontrato un illecito trattamento di degli indirizzi di posta elettronica ricavati dai *social network* per finalità di *marketing* (cd. *social spam*) in assenza del necessario e documentato consenso informato degli interessati. Nel vietare l'ulteriore trattamento (e riservandoci di contestare la violazione), abbiamo ribadito che la mera iscrizione a un *social network* non comporta la legittimità del trattamento dei dati conferiti allo stesso da parte di altri partecipanti ai fini dell'invio di informazioni commerciali [par. 10.4]

Ottobre

Abbiamo reso parere favorevole allo schema di decreto legislativo modificativo del Cad formulando alcune osservazioni al fine di adeguarne maggiormente il contenuto alla disciplina in materia di protezione dei dati personali [parr. 2.1.2] e segnalato criticamente al Presidente del Consiglio dei ministri l'istituzione, con disposizione inserita senza essere sottoposta al parere del Garante, di una Piattaforma Digitale Nazionale Dati, affidata in via sperimentale al Commissario straordinario per l'attuazione dell'agenda digitale, presso la quale verrebbero potenzialmente accentrati e duplicati, per finalità del tutto generiche, tutti i dati detenuti dalle pp.aa. [par. 4.2]

Alla luce delle numerose richieste di chiarimento su talune disposizioni del codice deontologico Sic e recependo gli orientamenti più recenti della Corte di cassazione,

siamo intervenuti per chiarire che: il creditore deve dare prova della ricezione da parte dell'interessato del preavviso di iscrizione al Sic; il periodo massimo di conservazione, in caso di inadempimenti non regolarizzati, non deve essere superiore ai cinque anni dalla scadenza del rapporto; poiché il codice deontologico si applica solo in presenza di una richiesta/rapporto di credito, e non nella fase propedeutica alla formulazione di una richiesta di finanziamento, nella predisposizione dell'informativa personalizzata SECCI si deve tener conto esclusivamente delle informazioni eventualmente rese dal consumatore, senza possibilità, in questa fase, di accedere al Sic [14.2.1]

Novembre

Abbiamo dichiarato illecito e disposto il divieto di ulteriore trattamento dei dati personali dei dipendenti del gestore del servizio postale universale effettuato mediante le nuove modalità di funzionamento del sistema di gestione delle attese allo sportello. Nel corso dell'istruttoria è emerso che la *consolle* di monitoraggio, con cui la società gestiva il sistema, consentiva a oltre 12.000 soggetti incaricati – con visibilità differenziata a livello nazionale e periferico – di accedere in tempo reale e in via continuativa ai dati relativi a tutte le postazioni, generando così un trattamento di dati personali non conforme ai principi di necessità, pertinenza e non eccedenza rispetto alle finalità perseguite oltre che in violazione della disciplina di settore in materia di controlli a distanza dei lavoratori [par. 13.3]

Considerata la specificità del settore e gli onerosi rischi gravanti sulle società di autonoleggio, è stata accolta una richiesta di verifica preliminare relativa al trattamento di dati personali connesso alla costituzione di una banca dati utilizzata esclusivamente per verificare l'eventuale censimento di soggetti che, nel tempo e a vario titolo, non abbiano provveduto alla restituzione dei veicoli noleggiati, con accesso consentito esclusivamente in caso di formale richiesta di stipula di un contratto di autonoleggio [par. 14.2.2]

Dicembre

In sede di verifica preliminare, abbiamo ritenuto lecito, individuando alcune prescrizioni, il trattamento effettuato mediante l'installazione di colonnine pubblicitarie che, dotate di sensori per la rilevazione delle immagini, consentono il trattamento dei dati così raccolti per fini di analisi dell'*audience* pubblicitaria. Al riguardo, è stato chiarito che il sistema consente di rilevare solo genericamente la presenza di un volto umano senza però identificarlo attraverso caratteristiche biometriche e che le immagini sono memorizzate solo localmente e temporaneamente, per essere sovrascritte dalle immagini successive [par. 14.3]

Considerata la perdurante reperibilità sul web di contenuti aventi un impatto "sproporzionatamente negativo" sulla sfera di un ricorrente residente al di fuori dell'Unione europea, anche in ragione del trattamento di dati potenzialmente sensibili che lo riguardano, abbiamo ordinato al gestore di un importante motore di ricerca, al fine di rendere effettiva la tutela, di rimuovere gli URL indicizzati con il nome del ricorrente sia nelle versioni europee che in quelle extra-europee (cd. deindicizzazione globale) [par. 19.3]

Abbiamo reso parere favorevole al Mise sullo schema di d.P.R. modificativo in materia di Registro pubblico delle opposizioni che prevede l'estensione della disciplina vigente anche alla posta cartacea con il trattamento dei dati personali relativi agli indirizzi postali. Tra l'altro, abbiamo segnalato l'opportunità di porre in essere campagne informative sulle modifiche introdotte, oltre che prevedere una disciplina transitoria che consenta a quanti interessati di opporsi all'utilizzo degli indirizzi presenti negli elenchi pubblici [par. 10.2]

Indice

Indice

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

1. Introduzione 3

2. Il quadro normativo in materia di protezione dei dati personali 9

2.1. Le novità normative con riflessi in materia di protezione dei dati personali 9

2.1.1. Le leggi di particolare interesse 9

2.1.2. I decreti legislativi 23

3. I rapporti con il Parlamento e le altre Istituzioni 27

3.1. Le audizioni del Garante in Parlamento 27

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

3.3. L'attività consultiva del Garante 28

3.3.1. I pareri sugli atti regolamentari e amministrativi del Governo 28

3.3.2. I pareri su norme di rango primario 30

3.4. L'esame delle leggi regionali 31

II – L'ATTIVITÀ SVOLTA DAL GARANTE

4. Il Garante e le amministrazioni pubbliche 35

4.1. I trattamenti di dati sensibili e giudiziari presso le amministrazioni pubbliche 35

4.2. La vigilanza sulle grandi banche dati pubbliche 37

4.3. La trasparenza amministrativa 38

4.3.1. L'accesso civico 38

4.3.2. La pubblicazione di dati personali online 45

4.4. L'istruzione scolastica 46

4.5. L'attività fiscale e tributaria 48

4.6. La videosorveglianza in ambito pubblico 51

4.7. I trattamenti effettuati presso regioni ed enti locali 54

4.8. La previdenza e l'assistenza sociale 57

5. La sanità e i dati genetici 58

5.1. I trattamenti per fini di cura 58

5.1.1. L'informativa e il consenso al trattamento dei dati sanitari 58

5.1.2. Il Fascicolo sanitario elettronico e il dossier *sanitario* 60

Indice

5.1.3. I referti e la documentazione sanitaria 62
5.1.4. La tutela della dignità della persona 63
5.1.5. Il trattamento di dati personali in relazione all'accertamento dell'infezione da HIV 63
5.2. I trattamenti di dati relativi alle condizioni di salute per fini amministrativi 64
5.2.1. Il trattamento dei dati personali nell'ambito dell'assolvimento degli obblighi vaccinali 66
5.3. I dati genetici 67

6. La ricerca scientifica e la statistica 69
6.1. La ricerca scientifica 69
6.2. La statistica e il censimento permanente 71

7. I trattamenti in ambito giudiziario e da parte delle Forze di polizia 74
7.1. I trattamenti in ambito giudiziario 74
7.2. Il controllo sul Ced del Dipartimento della pubblica sicurezza 76
7.3. L'individuazione dei trattamenti non occasionali effettuati con strumenti elettronici per finalità di polizia e le modalità di attuazione dei principi del Codice rispetto al trattamento dei dati effettuato per le finalità di polizia 76
7.4. La banca dati del Dna 78
7.5. Altri interventi riguardanti i trattamenti di dati da parte delle Forze di polizia 78
7.6. Il controllo sul sistema di informazione Schengen 80

8. L'attività giornalistica 82
8.1. I minori 83
8.2. La cronaca giudiziaria 83
8.3. La diffusione delle informazioni *online* 84

9. Il cyberbullismo 86

10. *Marketing*, profilazione e trattamento dei dati personali 87
10.1. Verifiche preliminari 87
10.2. *Marketing* 88
10.3. Telefonate indesiderate a contenuto promozionale: i controlli 91
10.4. *Spam* e raccolta di dati personali in internet 93
10.5. Invio per posta di comunicazioni a contenuto promozionale 97

Indice

11. Internet e servizi di comunicazione elettronica 99

11.1. Diffusione di dati personali in internet 99

11.2. Ricerche inverse 100

11.3. *Data breach* 100

11.4. Dati di traffico 105

12. Il trattamento dei dati personali da parte di movimenti politici 107

13. La protezione dei dati personali nel rapporto di lavoro pubblico e privato 109

13.1. Protezione dei dati personali e rapporto di lavoro 109

13.2. Il trattamento dei dati relativi ai dipendenti tramite sistemi di geolocalizzazione 109

13.3. Il trattamento dei dati personali mediante "altri strumenti": un sistema di gestione delle attese allo sportello 114

13.4. Il trattamento di dati personali mediante sistemi di videosorveglianza all'interno di aree particolari con rilevazione dell'audio 116

13.5. Il trattamento di dati biometrici 117

13.6. Il trattamento di dati giudiziari 118

13.7. Il trattamento di dati sanitari di familiari e congiunti del dipendente a fini di fruizione di permessi e congedi 119

14. Le attività economiche 121

14.1. Il settore bancario 121

14.2. Le banche dati interoperatore e i codici di deontologia nel settore economico/finanziario 121

14.2.1. I lavori di revisione del cd. codice Sic 121

14.2.2. Altre ipotesi di banche dati interoperatore 122

14.3. La videosorveglianza in ambito privato 124

14.4. Attività imprenditoriali: esonero dall'informativa 125

14.5. Attività imprenditoriali e nuove tecnologie 126

14.6. Indagine conoscitiva sui *big data* 128

15. L'attività di normazione tecnica internazionale e nazionale 129

16. Il trattamento dei dati personali nell'ambito del condominio 130

17. Il trasferimento dei dati personali all'estero 131

Indice

18. Il registro dei trattamenti 132

18.1. La notificazione 132

18.2. L'evoluzione delle notificazioni nel 2017 132

19. La trattazione dei ricorsi 134

19.1. I profili generali 134

19.2. I dati statistici 135

19.3. La casistica più significativa 136

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 146

21. L'attività ispettiva e le sanzioni 147

21.1. Gli ambiti dell'attività ispettiva 147

21.2. La collaborazione con la Guardia di finanza 148

21.3. I principali settori oggetto di controllo 149

21.4. I provvedimenti adottati a seguito dell'attività ispettiva 150

21.5. L'attività sanzionatoria 151

21.5.1. Le violazioni penali e i procedimenti relativi alle misure minime di sicurezza 151

21.5.2. Le sanzioni amministrative 153

22. Le relazioni comunitarie e internazionali 157

22.1. La cooperazione tra Autorità garanti nell'UE: il Gruppo Art. 29 157

22.2. La cooperazione delle Autorità di protezione dei dati nel settore libertà, giustizia e affari interni 168

22.3. Le conferenze delle Autorità su scala internazionale 171

22.4. La partecipazione ad altri comitati e gruppi di lavoro internazionali 172

23. L'attività di comunicazione e informazione e le relazioni con il pubblico 180

23.1. La comunicazione del Garante: profili generali 180

23.2. I prodotti informativi 182

23.3. I prodotti editoriali e multimediali 182
23.4. Le manifestazioni e le conferenze 184
23.5. L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi 186

24. Studi, documentazione e biblioteca 189
24.1. Il Servizio studi e documentazione 189
24.2. La biblioteca 190

III – L'UFFICIO DEL GARANTE

25. La gestione amministrativa e dei sistemi informatici 195
25.1. Il bilancio e la gestione economico-finanziaria 195
25.2. L'attività contrattuale, la logistica e la manutenzione degli immobili 197
25.3. L'organizzazione dell'Ufficio: il personale ed i collaboratori esterni 199
25.4. "Autorità trasparente" e adempimenti relativi alla disciplina anticorruzione 201
25.5. Il settore informatico e tecnologico 202

IV – I DATI STATISTICI 207

Avvertenza ed elenco delle abbreviazioni e degli acronimi più ricorrenti

La presente Relazione è riferita al 2017 e contiene talune notizie già anticipate nella precedente edizione nonché informazioni relative a sviluppi che si è ritenuto opportuno menzionare.

Acf	Arbitro per le controversie finanziarie
Aeegsi	Autorità per l'energia elettrica il gas e il sistema idrico
Aifa	Agenzia italiana del farmaco
Agcom	Autorità per le garanzie nelle comunicazioni
AgID	Agenzia per l'Italia digitale
All.	Allegato
Anac	Autorità nazionale anticorruzione
Anpr	Anagrafe nazionale della popolazione residente
Ans	Anagrafe nazione degli studenti
art.	articolo
Asl	Azienda sanitaria 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
Cad	Codice dell'amministrazione digitale
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)
Consob	Commissione nazionale per le società e la borsa
Corte EDU	Corte europea dei diritti dell'uomo
Cost.	Costituzione
d.d.l.	disegno di legge
d.l.	decreto-legge
d.lgs.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.G.p.	decreto Presidente Giunta provinciale
d.P.R.	decreto del Presidente della Repubblica
doc.	documento
es.	esempio

Fse	Fascicolo sanitario elettronico
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
Inapp	Istituto nazionale per l'analisi delle politiche pubbliche
Ivass	Istituto per la vigilanza sulle assicurazioni
IWGDPT	*International Working Group on Data Protection in Telecommunications*
l.	legge
lett.	lettera
Mef	Ministero dell'economia e delle finanze
Miur	Ministero dell'istruzione dell'università e della ricerca
Mise	Ministero dello sviluppo economico
n.	numero
Oam	Organismo degli agenti in attività finanziaria e dei mediatori creditizi
p.	pagina
p.a.	pubblica amministrazione
par.	paragrafo
Pec	posta elettronica certificata
provv.	provvedimento del Garante
r.d.	regio decreto
reg.	regolamento
RGPD	regolamento (UE) 679/2016
Rpd	Responsabile della protezione dei dati
Rpo	Registro pubblico delle opposizioni
Scipafi	Sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo con specifico riferimento al furto d'identità
sez.	sezione
Spid	Sistema pubblico dell'identità digitale
Ssn	Servizio sanitario nazionale
tab.	tabella
t.u.	testo unico
TFUE	Trattato sul funzionamento dell'Unione europea
Tulps	Testo unico delle leggi di pubblica sicurezza
UE	Unione europea
Uif	Unità di Informazione Finanziaria
Url	*Uniform resource locator*
v.	vedi

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

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

1 Introduzione

1.1. Nel saggio "*La rivoluzione della dignità*" (pubblicato postumo nel volume "*Vivere la democrazia*"), Stefano Rodotà – al cui ricordo e magistero quanti operano all'interno dell'Autorità sono affettuosamente legati – si domanda se, "nel mondo divenuto globale e segnato dalle innovazioni scientifiche e tecnologiche", "il principio di dignità è ancora un viatico". Se la dignità, cui già il Codice in materia di protezione dei dati personali faceva esplicito riferimento all'art. 2 (ed ora anche la Carta dei diritti fondamentali dell'Unione europea), possa costituire fondamento valoriale e baluardo sufficientemente solido "per evitare che la persona venga considerata una sorta di miniera a cielo aperto dove chiunque può attingere qualsiasi informazione e in tal modo costruire profili individuali, familiari, di gruppo, facendo così divenire la persona l'oggetto di poteri esterni, che possono falsificarla, costruirla in forme coerenti ai bisogni di una società della sorveglianza, della selezione sociale, del calcolo economico" (p. 62 s.).

1.2. È una delle questioni di fondo che attraversa la nostra società cui pure il Garante, nell'anno che abbiamo alle spalle e nell'attesa del pieno dispiegarsi delle potenzialità del nuovo quadro normativo costituito dal regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679, RGPD), guarda con accresciuta preoccupazione. Non per mero spirito speculativo o sulla base di considerazioni astratte, ma costretto dall'osservazione dei dati di realtà: muovendo anzitutto da derive normative che, anche nell'ordinamento italiano, sembrano dirigersi verso massive ed inedite concentrazioni di informazioni personali, sì da revocare in dubbio l'effettività dei principi fondanti, vecchi e nuovi, in materia di protezione dei dati personali, quelli di minimizzazione, proporzionalità, finalità, *privacy by design* e *by default*. Freschi di stampa nel RGPD, sono tutti messi alla corda da disposizioni recenti che, ad esempio, fissano in sei anni i tempi di conservazione dei dati di traffico (cfr. art. 24, l. 22 novembre 2017, n. 167), peraltro in aperto contrasto con la giurisprudenza della Corte di giustizia (par. 11.4); prevedono, all'art. 50-*ter* del Cad (decreto legislativo 7 marzo 2005, n. 82), la realizzazione della Piattaforma Digitale Nazionale Dati, affidata in via sperimentale al Commissario straordinario per l'attuazione dell'agenda digitale, presso la quale, "con un impatto senza precedenti", verrebbero potenzialmente accentrati e duplicati, per finalità del tutto generiche, tutti i dati personali detenuti dalle pp.aa. (par. 4.2); introducono censimenti perma-

nenti (cfr. commi 227, 228 e 229, della legge 27 dicembre 2017, n. 205, recante il bilancio di previsione dello Stato per l'anno finanziario 2018), mediante la centralizzazione presso l'Istat di rilevanti archivi nella disponibilità degli enti pubblici, compresa l'Anagrafe tributaria (par. 6.2). Innovazioni legislative che il Garante ha criticamente portato all'attenzione di Parlamento e Governo, sollecitandone il ripensamento (cfr., le segnalazioni del 22 dicembre 2017, doc. web n. 7464029, 22 gennaio 2018, doc. web n. 8456134 e 7 novembre 2017, doc. web n. 7447536).

Non diversamente, con grande attenzione è seguita l'iniziativa, conseguente all'accordo siglato tra la Presidenza del Consiglio dei ministri e una multinazionale dell'Ict, che comporterebbe la comunicazione a quest'ultima di dati personali relativi a prestazioni sanitarie e farmaceutiche degli assistiti dal Ssn detenuti dalle regioni e dall'Aifa (par. 5.2).

1.3. Così, per decifrare se ed in quale misura la rivoluzione digitale metta a repentaglio diritti e libertà fondamentali, il Garante è venuto interrogandosi su rischi ed opportunità che accompagnano le tecniche innovative di interrogazione ed analisi di estesi (e differenziati) *dataset*, per meglio comprendere se i cd. *big data* sottendano, come con felice formula è stato detto, anche *big risks*. Di qui il *focus* sul tema nel 2017, dapprima dedicando ad esso il tradizionale convegno in occasione della "Giornata europea della protezione dei dati personali" (i cui atti sono raccolti nel volume disponibile al doc. web n. 6494810); quindi avviando, d'intesa con l'Autorità garante per la concorrenza e il mercato e l'Autorità per le garanzie nelle comunicazioni, un'indagine conoscitiva congiunta dedicata al tema, ancora in corso (par. 14.6).

1.4. E se è l'aspetto "dimensionale" che immediatamente salta agli occhi – con riguardo ai volumi dei dati personali accumulati e trattati (destinati ad aumentare vertiginosamente con la diffusione dell'*Internet of Things*) e alla irrilevanza pratica della dimensione spazio-temporale dei trattamenti (si pensi al *cloud computing*) –, non può stupire (anche se preoccupa) che l'azione sistematica di controllo posta in essere dall'Autorità nell'assolvimento dei propri compiti istituzionali – anche con la collaborazione della Guardia di finanza (par. 21.2) – abbia fatto a sua volta emergere violazioni esse pure di dimensioni ragguardevoli.

Ciò è accaduto, ad esempio, a seguito dell'azione di contrasto tenacemente portata avanti nei confronti del fenomeno del cd. *telemarketing* selvaggio – piaga da tempo segnalata dal Garante (già a partire dalla Relazione 2008, con specifico riferimento al settore dei servizi telefonici, e quindi presente senza soluzione di continuità nell'agenda dell'Autorità) – che, all'esito di un ciclo di intense attività ispettive (talune delle quali al di fuori dei confini nazionali, prestando assistenza all'Autorità di controllo albanese), ha condotto all'adozione di provvedimenti inibitori di tutto rilievo, con l'accertamento di milioni di contatti commerciali effettuati in violazione di legge, e la conseguente attivazione dei relativi procedimenti sanzionatori (par. 10.2 e 10.3). Peraltro, tale ambito, in uno stretto arco temporale, ha registrato, circostanza non casuale, reiterati interventi da parte del legislatore sull'attività degli operatori di *call center* (e la loro delocalizzazione) nel tentativo di arginarne le distorsioni e gli effetti dannosi (per i singoli e, al fondo, per le stesse realtà imprenditoriali, oltre che per le negative ripercussioni occupazionali) (par. 2.1.1).

E l'attività ispettiva si è incentrata anche su altri fenomeni di notevole rilevanza, con la successiva adozione da parte del Garante di provvedimenti contenenti articolate prescrizioni, talora con ricadute di natura sanzionatoria (par. 21.4): basti menzionare, con riguardo ai profili connessi alla sicurezza informatica, i *data breach*

oggetto di accertamento presso alcuni dei principali operatori di telefonia nazionale (par. 11.3), oltre che presso pubbliche amministrazioni (par. 4.2), o alle prescrizioni impartite ad un movimento politico, in merito a delicati profili di sicurezza informatica la cui compromissione, in ragione del peculiare ambito del trattamento, potrebbe riverberarsi nell'esercizio di prerogative di rilevanza costituzionale da parte degli aderenti (cap. 12).

Particolarmente significativi per l'entità delle sanzioni contestate i cinque provvedimenti collegiali di ordinanza-ingiunzione, adottati nei confronti di altrettante società di *money transfer*, con i quali sono stati definiti complessivamente 1.081 procedimenti sanzionatori, con conseguente applicazione di sanzioni per oltre 11.000.000 euro (par. 21.5.2).

1.5. Continuano a ripetersi gli interventi dell'Autorità nei contesti direttamente connessi alla vita delle persone. Anzitutto in relazione ai trattamenti effettuati nel rapporto di lavoro, ambito nel quale il Garante ha ritenuto che determinati dispositivi (in particolare quelli provvisti di funzionalità di geolocalizzazione) e sistemi tecnologici (ad esempio preordinati alla gestione di attività di *call center* o della gestione delle attese della clientela allo sportello) debbano qualificarsi quali strumenti di controllo e non, invece, strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, con conseguente piena applicazione, anche dopo le modifiche apportata dal cd. *Jobs Act*, della procedura di garanzia prevista dalla disciplina di settore in materia di controlli a distanza (par. 13.2).

Anche per recepire un orientamento espresso dalla Corte di cassazione – che ha stabilito il principio di diritto secondo cui "l'onere di preventivo avvertimento, di cui alla norma dell'art. 4, comma 7 della delib. Garante Privacy 16 novembre 2004, n. 8, risulta assolto solo quando la relativa dichiarazione abbia effettivamente raggiunto il domicilio del destinatario, salva comunque restando l'eventualità che quest'ultimo provi di essere stato, senza sua colpa, nell'impossibilità di averne notizia" (Sez. I civ., ord., 13 giugno 2017, n. 14685) – il Garante, con proprio provvedimento, ha espresso alcuni chiarimenti sulle disposizioni del codice deontologico Sic che generavano da tempo considerevoli dubbi interpretativi e applicativi (par. 14.2.1).

Ancora numerose sono le decisioni aventi ad oggetto la deindicizzazione dai motori di ricerca di notizie riferite a singoli, nelle quali il Garante ha continuato a ritenere applicabile la disciplina di protezione dei dati a gestori dei motori di ricerca stabiliti al di fuori dell'Unione europea, ritenendo altresì, in uno dei casi portati alla propria attenzione (cfr. provv. 21 dicembre 2017, n. 557, doc. web n. 7465315), che la richiesta di rimozione di alcuni URL dovesse essere estesa a tutti i risultati di ricerca, sia nelle versioni europee che extra-europee del motore di ricerca (par. 19.3).

1.6. Va inoltre evidenziata l'intensa attività di confronto e approfondimento con il Ministero dell'interno, in clima di piena collaborazione istituzionale, infine confluita nei pareri resi dal Garante (par. 7.3): anzitutto in relazione ad uno schema di decreto ministeriale, previsto dall'art. 53 del Codice, recante l'individuazione dei trattamenti non occasionali effettuati per finalità di polizia eseguiti con strumenti elettronici, che in termini di trasparenza (e quindi di democraticità) nel trattamento delle informazioni consente alla collettività di conoscere quante e quali sono le banche dati gestite dalle Forze di polizia e quali sono le operazioni che possono essere effettuate loro tramite. Poi, con riguardo a due schemi di decreto del Presidente della Repubblica che, secondo quanto previsto dall'art. 57 del Codice, disciplinano le modalità di attuazione dei principi del Codice al trattamento dei dati effettuato

per le finalità di polizia: il primo, a contenuto generale, riferito a tutti i trattamenti effettuati da organi, uffici o comandi di polizia; il secondo, concernente i trattamenti effettuati dal Centro elaborazioni dati della Polizia di Stato (pareri 23 febbraio 2017, n. 74, doc. web n. 6197012, e 2 marzo 2017 n. 86, doc. web n. 6197365).

1.7. Se si sono così riassunti, per sommi capi, alcuni dei settori interessati dagli interventi del Garante, merita pure segnalare l'attribuzione da parte del legislatore di nuovi compiti in capo ad esso (peraltro scanditi da una rigorosa tempistica e senza assegnazione di maggiori risorse), sia in relazione al grave fenomeno (che pare essere in preoccupante ascesa) del cyberbullismo (cap. 9), sia in relazione alla diversa materia dell'accesso civico, rispetto alla quale il Garante nel corso del 2017 ha reso – ai sensi dell'art. 5, commi 7 e 8, d.lgs. 14 marzo 2013, n. 33, nei tempi previsti (10 giorni) – numerosi pareri a vantaggio dei responsabili della prevenzione della corruzione o a difensori civici chiamati ad individuare, nei casi in concreto loro sottoposti in sede di riesame, il corretto punto di equilibrio tra il rispetto del diritto alla riservatezza e alla protezione dei dati personali di quanti interessati dalle istanze di accesso generalizzato e l'interesse alla trasparenza dell'attività amministrativa (par. 4.3.1).

1.8. Materia quest'ultima, oggetto di intervento in più occasioni da parte del Garante (come risulta ormai da ciascuna Relazione di attività, a partire da quella del 2010, p. 54 s.) e anche nel 2017 contrassegnata dall'adozione di ripetuti provvedimenti inibitori in presenza dell'illecita diffusione (nell'intento di dare attuazione alla disciplina di trasparenza) di dati riferiti alle condizioni di salute dei singoli su siti web istituzionali (par. 4.3.2). Rispetto alla stessa merita segnalare, con specifico riferimento all'attuazione di taluni degli obblighi di pubblicità concernenti i dati riferibili ai titolari di incarichi dirigenziali, l'ordinanza del T.A.R. Lazio, sede di Roma, sez. I-*quater*, del 19 settembre 2017, n. 9828, con la quale è stata dichiarata rilevante e non manifestamente infondata, per contrasto con gli artt. 117, comma 1, 3, 2 e 13 Cost., la questione di legittimità costituzionale dell'art. 14, comma 1-*bis* e comma 1-*ter*, d.lgs. n. 33/2013 (inseriti dall'art. 13, comma 1, lett. *c*), d.lgs. 25 maggio 2016, n. 97), nella parte in cui prevedono che le pubbliche amministrazioni pubblichino i dati di cui all'art. 14, comma 1, lett. *c*) ed *f*) dello stesso decreto legislativo anche per i titolari di incarichi dirigenziali, rimettendola alla Corte costituzionale.

1.9. Ma nel 2017, con un crescendo nell'anno in corso, si sono sovrapposte alle "ordinarie" attività facenti capo all'Autorità, una pluralità di azioni, in varia forma volte a favorire un approccio progressivo alla nuova cornice normativa eurounitaria entro la quale trovano sede elettiva (ancorché non esclusiva) le disposizioni che regoleranno in futuro la materia della protezione dei dati: il ricordato RGPD e la direttiva 2016/680 del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo 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.

Anzitutto con il lavoro costante dell'Ufficio nell'ambito dei vari sottogruppi di lavoro del Gruppo Art. 29, culminati con l'adozione di linee guida e documenti di orientamento, dedicati in particolare ai temi di più immediato impatto nell'applicazione del RGPD: si pensi alle linee guida dedicate alla portabilità dei dati, alla figura del responsabile della protezione dei dati, alla designazione dell'"Autorità

capofila", al *Data protection impact assessment* (Dpia), alle materie della profilazione e delle decisioni automatizzate, del consenso, della trasparenza, della notifica delle violazioni di dati personali, delle sanzioni amministrative nonché ai documenti in materia di trasferimenti di dati all'estero. Nondimeno merita di essere ricordato anche il documento in materia di protezione dei dati e *law enforcement*, incentrato sulla direttiva 2016/680 (v. *amplius* cap. 22).

1.10. E molteplici iniziative sono state intraprese dall'Autorità anche sul versante nazionale. Tra le più significative merita ricordare la campagna d'informazione e di comunicazione in vista dell'applicazione del RGPD rivolta sia alla collettività – con la diffusione di opuscoli, pagine informative, infografiche e FAQ, distribuiti in occasione di incontri pubblici e convegni, nonché sulle reti Rai (spot radio e tv), sul web e sui canali *social*, grazie ai profili istituzionali aperti dal Garante (par. 23.1) –, come pure mirata a sensibilizzare i principali soggetti pubblici. In quest'ultimo ambito, il 24 maggio 2017 è stata inviata una comunicazione ai vertici delle amministrazioni centrali e locali, a firma del Presidente dell'Autorità, per evidenziare l'importanza di avviare quanto prima le attività di recepimento dei nuovi adempimenti previsti dal RGPD, indicando quali priorità: 1) la designazione di un responsabile della protezione dei dati; 2) l'istituzione del registro delle attività di trattamento; 3) la definizione della procedura di gestione delle violazioni di dati personali (*data breach*). In questa prospettiva, le amministrazioni destinatarie della comunicazione sono state invitate a far partecipare propri referenti a tre incontri organizzati (il 12, 16 e 20 giugno) presso la sede del Garante allo scopo di "ascoltare" le pp.aa. e ricevere richieste e suggerimenti nonché valutare le esigenze legate all'applicazione del regolamento: hanno aderito all'iniziativa 136 dirigenti e funzionari, in rappresentanza di 64 soggetti pubblici. Sulla base degli elementi acquisiti, quale *follow up* di questa attività, sono state elaborate le FAQ sul Responsabile della protezione dei dati (Rpd) in ambito pubblico, ad integrazione di quelle adottate dal Gruppo Art. 29, rese pubbliche sul sito dell'Autorità il 15 dicembre 2017 (doc. web n. 7322110).

In una seconda fase (a partire dal mese di novembre), anche sulla base delle informazioni acquisite nel mese di giugno e dell'evoluzione del quadro giuridico a seguito dell'adozione delle linee guida del Gruppo Art. 29, sono stati organizzati ulteriori incontri, questa volta presso le amministrazioni centrali e territoriali, aperti ai rappresentanti di tutti i soggetti pubblici e, nel limite dei posti disponibili, anche ai privati, con l'obiettivo di fornire supporto al cambiamento. I primi tre incontri si sono tenuti il 7 novembre a Roma, con la collaborazione della Banca d'Italia, il 4 dicembre, con la collaborazione della Regione Lombardia, a Milano, il 15 gennaio 2018, con la collaborazione della Regione Puglia, a Bari. Il ciclo si è concluso con un ulteriore incontro, organizzato in collaborazione con il Cineca – Consorzio con il quale, anche nell'anno in corso, è continuata una proficua cooperazione istituzionale –, dedicato al mondo delle università, tenutosi a Roma presso il Centro nazionale delle ricerche. A latere delle iniziative principali si sono tenuti due ulteriori seminari: uno, su richiesta della Camera dei deputati, diretto agli organi di rilievo costituzionale, e l'altro, a Roma, presso Sogei s.p.a., volto ad esaminare l'impatto del RGPD nel settore della fiscalità. Tutti gli eventi sono stati caratterizzati da un elevato interesse e partecipazione, hanno coinvolto complessivamente circa 3.000 persone e, in considerazione del fatto che le richieste di partecipazione hanno ecceduto i posti disponibili, gli stessi sono stati anche trasmessi in diretta *streaming*.

1.11. Incontri e interazioni hanno riguardato anche il settore privato, anzitutto con l'invito rivolto ad Abi, Ania e Confindustria per promuovere tavoli di confronto

sui problemi del RGPD; ma numerose sono state le iniziative formative cui l'Ufficio ha preso parte (ad esempio, con Assaeroporti, Assorevi, Assogestioni, Confcommercio, Confapi, Ancic, Federfarma, etc.). Altro ambito di attività ha riguardato i meccanismi, introdotti dal RGPD (artt. 42 e 43), per la certificazione della protezione dei dati personali nonché di sigilli e marchi, allo scopo di dimostrare la conformità dei trattamenti posti in essere. Su questi temi l'Autorità ha lavorato congiuntamente alle altre autorità di controllo europee allo scopo di delineare, nel rispetto del RGPD, un quadro comune di criteri per accreditare gli organismi di certificazione e per la certificazione dei trattamenti.

Al fine di confrontarsi e acquisire elementi utili all'individuazione dei requisiti aggiuntivi per l'accreditamento e dei criteri di certificazione, è stato inoltre istituito, in ambito nazionale, un tavolo di lavoro con Accredia, ossia l'Ente unico nazionale di accreditamento designato dal Governo italiano ai sensi del regolamento (UE) 765/2008. In questa cornice di riferimento, è stata colta l'occasione per puntualizzare che le certificazioni di persone, nonché quelle emesse in materia di *data protection*, eventualmente rilasciate *medio tempore* in Italia, sebbene possano costituire una guarentigia verso gli interessati (implicando l'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento), non possono tuttavia definirsi, a legislazione vigente, "conformi agli artt. 42 e 43 del regolamento (UE) 2016/679", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione; tutto ciò al fine di indirizzare correttamente, in questa prima fase di applicazione della normativa, le attività svolte dai soggetti a vario titolo interessati nell'ambito considerato (cfr. comunicato stampa 18 luglio 2017, doc. web n. 6621723).

1.12. In conclusione: ad oltre 20 anni dall'entrata in vigore della prima disciplina di protezione dei dati personali nel nostro ordinamento (l. n. 675/1996), molte sono le attese e le speranze riposte nella nuova cornice regolatoria della quale (non senza fatica e resistenze) l'Unione europea si è dotata per tenere il passo dell'innovazione tecno-scientifica, anche grazie all'operato delle autorità di protezione dei dati personali e con una rinnovata responsabilizzazione (*accountability*) di tutti gli attori sociali. Il processo, che ha immediati riflessi sul piano economico-sociale ed ampia eco su scala globale, peraltro, è ancora in corso in relazione alla proposta di regolamento sulla protezione della vita privata e le comunicazioni elettroniche (cd. *e-privacy*).

L'obiettivo per tutti è chiaro e traspare dal Preambolo della Carta dei diritti fondamentali dell'Unione europea, che vuole "la persona al centro della sua azione"; perché, anche nel prisma della dimensione digitale, l'"*homo numericus*" possa continuare ad essere "*homo dignus*". Si tratta di avere la forza e la volontà di perseguirlo.

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 2017 sono stati approvati numerosi provvedimenti normativi che hanno riflessi in materia di protezione dei dati personali. Fra questi, al fine di offrirne una ricognizione, pur sintetica ma tale da rendere conto dell'ampiezza e dell'eterogeneità delle materie che rientrano nell'area di interesse dell'Autorità, si menzionano in particolare:

Legge di bilancio 2018

1) la legge 27 dicembre 2017, n. 205 recante il bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020. Molteplici sono i commi di questa legge che risultano di interesse per la materia della protezione dei dati personali. Innanzitutto, vanno ricordati i commi 1020 e seguenti con i quali sono state introdotte ulteriori disposizioni ai fini dell'adeguamento dell'ordinamento italiano al nuovo quadro normativo dell'Unione europea in materia di trattamento dei dati personali. Tali disposizioni si aggiungono a quelle contenute nella legge n. 163/2017 (Legge di delegazione europea) che, all'art. 13, contiene i criteri di delega per il suddetto adeguamento (cfr. par. 2.1, punto 6). Il comma 1020 ribadisce il ruolo di garanzia dell'Autorità, disponendo che "il Garante per la protezione dei dati personali assicura la tutela dei diritti fondamentali e delle libertà dei cittadini". Il successivo comma 1021, dispone che il Garante, con proprio provvedimento da adottare entro due mesi dalla data di entrata in vigore della medesima legge n. 205/2017, provveda a:

a) disciplinare le modalità attraverso le quali il Garante stesso monitora l'applicazione del RGPD e vigila sulla sua applicazione;
b) disciplinare le modalità di verifica, anche attraverso l'acquisizione di informazioni dai titolari dei dati personali trattati per via automatizzata o tramite tecnologie digitali, della presenza di adeguate infrastrutture per l'interoperabilità dei formati con cui i dati sono messi a disposizione dei soggetti interessati, sia ai fini della portabilità dei dati ai sensi dell'art. 20 del RGPD, sia ai fini dell'adeguamento tempestivo alle disposizioni del medesimo;
c) predisporre un modello di informativa da compilare a cura dei titolari di dati personali che effettuano un trattamento fondato sull'interesse legittimo che preveda l'uso di nuove tecnologie o di strumenti automatizzati;
d) definire linee guida o buone prassi in materia di trattamento dei dati personali fondato sull'interesse legittimo del titolare.

Il comma 1022, al fine di dettare disposizioni integrative per adeguare al RGPD l'ordinamento interno, prescrive che il titolare del trattamento individuato ai sensi dell'art. 4, punto 7), del RGPD, ove tratti dati personali mediante l'uso di nuove tecnologie o di strumenti automatizzati sulla base di un interesse legittimo, deve darne tempestiva comunicazione all'Autorità. A tal fine, prima di procedere al trattamento, il titolare dei dati dovrà inviare all'Autorità un'informativa relativa all'oggetto, alle finalità e al contesto del trattamento, utilizzando il modello predisposto e reso disponibile dalla medesima Autorità. In tal caso (comma 1023) il Garante può disporre una breve moratoria del trattamento per ricevere ulteriori elementi e, ove rilevi che dal trattamento possa derivare comunque una lesione dei diritti e delle

libertà degli interessati, può inibirlo. In caso di mancata risposta da parte del Garante nel termine di quindici giorni lavorativi dall'invio dell'informativa, il titolare può procedere al trattamento (silenzio-assenso).

Il comma 1024, fa obbligo al Garante di dar conto nella Relazione annuale dell'attività svolta ai sensi del comma 1023 e dei provvedimenti conseguentemente adottati: a questo proposito indicazioni preliminari sono state fornite con il provv. 22 febbraio 2018, n. 121 (doc. web n. 8080493), anche in ragione del mancato esercizio della delega per l'attuazione delle disposizioni del Regolamento di cui alla legge n. 205/2017 (al tempo dell'adozione del provvedimento).

In considerazione delle ulteriori attribuzioni è stato autorizzato uno stanziamento di 2 milioni di euro annui a decorrere dall'anno 2018 (comma 1025).

Censimenti permanenti

Particolare attenzione hanno destato alcune disposizioni in materia di censimenti permanenti, ivi incluso quello della popolazione e delle abitazioni (cfr. commi 227, 228 e 229). In particolare, al comma 228 della legge viene previsto che gli archivi di tutti gli enti pubblici, compresa l'Anagrafe tributaria, confluiscano in un unico grande *database* dell'Istat; dati sui minori, sulle condizioni di salute, sulla situazione tributaria e addirittura sui consumi energetici di luce e gas, tutto raccolto in un unico "archivio" centrale, materialmente situato presso l'Istat. Il Garante è quindi intervenuto nel corso dell'*iter* parlamentare segnalando (criticamente) l'incongruenza di dette disposizioni in materia di censimenti permanenti rispetto alle norme sulla protezione dei dati personali nazionali ed europee (nota del Presidente 7 novembre 2017, doc. web n. 7447536, sulla quale, con un maggiore grado di dettaglio, v. infra par. 6.2). A seguito della menzionata segnalazione è stata introdotta, al comma 227, lett. *e*), una specifica menzione del Garante tra le Autorità chiamate a dare un parere in merito alle modalità di effettuazione del trattamento dei dati. È stato altresì previsto che per poter effettuare il trattamento dei dati sui consumi, venga adottato un protocollo d'intesa tra Istat e Acquirente Unico s.p.a. sentite l'Autorità per l'energia elettrica il gas ed il settore idrico, il Garante per la protezione dei dati personali e l'Autorità garante della concorrenza e del mercato.

Aeegsi

Anche in altre disposizioni si prevede un intervento consultivo del Garante. Ciò in particolare riguarda i commi 7 ed 8, che, rispettivamente, introducono una nuova denominazione e nuove funzioni di regolazione e controllo per l'Autorità per l'energia elettrica il gas ed il sistema idrico (Aeegsi) e stabiliscono che entro il 1° luglio 2019, il soggetto gestore del Sistema informatico integrato per la gestione dei flussi informativi relativi ai mercati dell'energia elettrica e del gas "provveda agli adeguamenti necessari per permettere ai clienti finali di accedere attraverso il Sistema medesimo ai dati riguardanti i propri consumi, senza oneri a loro carico". Gli adeguamenti attuativi della predette disposizioni saranno adottati con deliberazione dell'Autorità per l'energia elettrica, il gas e il sistema idrico, "nel rispetto delle norme in materia di protezione dei dati personali, sentito il parere del Garante per la protezione dei dati personali".

Archivi notarili

Il comma 495 interviene sulla gestione dell'amministrazione degli archivi notarili, prevedendo che con uno o più decreti del Ministro della giustizia, di concerto con il Ministro dell'economia e delle finanze e il Ministro per la semplificazione e la pubblica amministrazione, sentiti il Consiglio nazionale del notariato, il Garante e l'Agenzia per l'Italia digitale, "sono determinate le modalità di formazione e trasmissione telematica delle copie degli atti e dei versamenti, la conservazione, la ricerca e la consultazione dei documenti e dei dati inseriti nell'archivio centrale informatico".

DAT

Nella medesima legge viene prevista, ai commi 418 e 419, rispettivamente, l'istituzione presso il Ministero della salute di una banca dati destinata alla registrazione

delle disposizioni anticipate di trattamento (DAT), introdotte con la l. 22 dicembre 2017, n. 219 (cfr. capoverso successivo), attraverso le quali ogni persona maggiorenne e capace di intendere e di volere, in vista di un'eventuale futura incapacità di autodeterminarsi, può esprimere le proprie volontà in materia di trattamenti sanitari nonché il consenso o il rifiuto rispetto ad accertamenti diagnostici o scelte terapeutiche e a singoli trattamenti sanitari. Si prevede che "entro centottanta giorni dalla data di entrata in vigore della legge (DAT), con decreto del Ministro della salute, previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano e acquisito il parere del Garante per la protezione dei dati personali, sono stabilite le modalità di registrazione delle DAT presso la banca dati di cui al comma 418".

2) Legge 22 dicembre 2017, n. 219, recante le norme in materia di consenso informato e di disposizioni anticipate di trattamento.

DAT e consenso informato

La legge richiama i diritti alla vita, alla salute, alla dignità e all'autodeterminazione della persona, dettando la disciplina del consenso informato – fondamento della relazione di cura e di fiducia tra paziente e medico – in relazione ai trattamenti sanitari ed agli accertamenti diagnostici.

Ogni paziente capace di agire ha il diritto di rifiutare qualsiasi accertamento diagnostico o trattamento sanitario indicato dal medico per la sua patologia o singoli atti del trattamento stesso così come il diritto di revocare in qualsiasi momento il consenso precedentemente prestato, anche qualora la revoca comporti l'interruzione del trattamento.

Il consenso informato, acquisito nei modi e con gli strumenti più consoni alle condizioni del paziente, ovvero il rifiuto o la revoca del consenso sono documentati in forma scritta o attraverso videoregistrazioni o, per la persona con disabilità, attraverso dispositivi che le consentano di comunicare. Ferma restando la possibilità per il paziente di modificare la propria volontà, l'accettazione, la revoca e il rifiuto sono annotati nella cartella clinica e nel fascicolo sanitario elettronico (art. 1, commi 4 e 5).

La legge estende e amplifica il diritto alla "valorizzazione" delle capacità di comprensione e di decisione, nel rispetto dei diritti alla vita, alla salute, alla dignità e all'autodeterminazione della persona, anche con riguardo ai minori di età e agli incapaci, prevedendo che, al fine di porli in condizione di esprimere le proprie volontà, a questi ultimi le informazioni sulle scelte relative alla salute siano fornite in modo consono alle proprie capacità.

Come si è anticipato, l'art. 4 della legge introduce l'istituto delle disposizioni anticipate di trattamento, concernenti le proprie volontà in materia di trattamenti sanitari, accertamenti diagnostici e scelte terapeutiche, espresse per l'ipotesi di una futura incapacità di autodeterminarsi. Tale volontà può essere espressa da ogni persona maggiorenne e capace di intendere e volere, dopo aver acquisito adeguate informazioni mediche sulle conseguenze delle proprie scelte; l'interessato può indicare una persona di fiducia, denominata fiduciario, che (nel caso in cui sopravvenga l'incapacità suddetta) faccia le proprie veci e lo rappresenti nelle relazioni con il medico e con le strutture sanitarie.

Le disposizioni anticipate di trattamento, redatte per atto pubblico o mediante scrittura privata autenticata ovvero mediante scrittura privata, devono essere consegnate presso l'ufficio dello stato civile del proprio comune di residenza – che provvede ad annotarle in apposito registro – oppure, qualora le condizioni fisiche del paziente non permettano il ricorso alle suddette forme, possono essere espresse attraverso videoregistrazione o dispositivi che consentano alla persona con disabilità di comunicare. Come già visto nel precedente paragrafo, il comma 418 della legge

di bilancio ha previsto l'istituzione presso il Ministero della salute di una banca dati destinata alla registrazione delle DAT, mentre nel comma 419 della medesima legge si prevede che – con decreto del Ministro della salute, previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano e acquisito il parere del Garante – vengano stabilite le modalità di registrazione delle DAT presso la istituita banca dati.

La legge dispone inoltre che le regioni che adottano modalità telematiche o informatiche di gestione dei dati dell'iscritto al Servizio sanitario nazionale possano regolamentare la raccolta di copia delle DAT, compresa l'indicazione del fiduciario, ed il loro inserimento nella banca dati, lasciando in ogni caso al firmatario la libertà di scegliere se depositarne anche una copia presso la regione o indicare dove esse siano reperibili.

Si prevede anche che la disciplina in materia di consenso informato e di disposizioni anticipate di trattamento si applichi ai documenti idonei ad esprimere le volontà del disponente in merito ai trattamenti sanitari, depositati presso il comune di residenza o presso un notaio prima della data di entrata in vigore della legge e che il Ministro della salute trasmetta alle Camere, entro il 30 aprile di ogni anno, a decorrere dall'anno successivo a quello in corso alla data di entrata in vigore della legge, sulla base delle informazioni fornite dalle regioni, una relazione sull'applicazione della medesima.

Legge europea 2017

3) Legge 20 novembre 2017, n. 167, recante le disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017.

La legge incide significativamente sul Codice, ed in particolare sulle seguenti disposizioni:

Art. 132, commi 1 e 1-*bis*: l'art. 24 della legge in parola, rubricato "termini di conservazione dei dati di traffico telefonico e telematico", prevede che "in attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo, al fine di garantire strumenti di indagine efficaci in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-*quater*, e 407, comma 2, lettera *a*), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-*bis*, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-*bis*, del Codice in materia di protezione dei dati personali, di cui al d.lgs. 30 giugno 2003, n. 196". Anche in questo caso, riprendendo quanto affermato dalla Corte di Giustizia dell'Unione europea, Grande Camera, con la sentenza 21 dicembre 2016 (cause riunite C-203/15 e C-698/15), il Garante è intervenuto per segnalare che il termine di 6 anni fissato nel testo per la conservazione dei dati di traffico telefonico e telematico e dei dati relativi alle chiamate senza risposta appare in palese contrasto con l'ordinamento dell'Unione europea e con la giurisprudenza della Corte di giustizia; questi ultimi precludono infatti una raccolta generalizzata e indiscriminata dei dati di traffico telefonico e telematico, in quanto non proporzionata alle esigenze investigative e al nucleo essenziale del diritto alla protezione dati, sì da non potersi ritenere giustificata in una società democratica (cfr. nota del Presidente 22 dicembre 2017, doc. web n. 7464029). Ne deriva che è tuttora possibile prevedere obblighi di raccolta dei dati ma esclusivamente per obiettivi specifici, al solo fine di perseguire reati gravi, purché tali

obblighi siano limitati temporalmente in misura proporzionata alle esigenze investigative e riguardino le sole informazioni a ciò strettamente necessarie (sul tema v. pure *infra* par. 11.4).

Art. 29, nuovo comma 4-*bis*: l'art. 28 della legge in parola, rubricato "modifiche al d.lgs. 30 giugno 2003, n. 196", aggiunge all'art. 29 del Codice (sul responsabile del trattamento) un comma 4-*bis*, che di fatto recepisce, in parte, modalità di designazione, caratteristiche soggettive e ruolo della figura del responsabile del trattamento previsto dal RGPD, e che inoltre modifica il comma 5 dello stesso, al fine di coordinare gli obblighi del responsabile e i rapporti tra titolare e responsabile al predetto comma 4-*bis*;

Art. 110-*bis*: la legge aggiunge al Codice il nuovo art. 110-*bis* in materia di riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici prevedendo, con disposizione che ha suscitato molteplici perplessità (cfr. par. 6.1), che "nell'ambito delle finalità di ricerca scientifica ovvero per scopi statistici può essere autorizzato dal Garante il riutilizzo dei dati, anche sensibili, ad esclusione di quelli genetici, a condizione che siano adottate forme preventive di minimizzazione e di anonimizzazione dei dati ritenute idonee a tutela degli interessati. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del riutilizzo dei dati, anche sotto il profilo della loro sicurezza".

4) Legge 30 novembre 2017, n. 179, recante disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato.

Whistleblowing

La nuova legge ha come obiettivo principale quello di garantire una tutela adeguata ai lavoratori, assicurando agli stessi un'ampia tutela della riservatezza. In particolare, le nuove norme modificano l'art. 54-*bis* del Testo unico del pubblico impiego stabilendo che il dipendente che segnala al responsabile della prevenzione della corruzione dell'ente o all'Anac o ancora all'autorità giudiziaria ordinaria o contabile le condotte illecite o di abuso di cui sia venuto a conoscenza in ragione del suo rapporto di lavoro, non può essere, per motivi collegati alla segnalazione, soggetto a sanzioni, demansionato, licenziato, trasferito o sottoposto a altre misure organizzative che abbiano un effetto negativo sulle condizioni di lavoro.

La nuova disciplina prevede la nullità dei licenziamenti ritorsivi o discriminatori nei confronti del soggetto segnalante, nonché del mutamento di mansioni e di ogni altra misura ritorsiva o discriminatoria adottata nei suoi confronti dal datore di lavoro. Sarà onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari o a demansionamenti, licenziamenti o trasferimenti – successivi alla presentazione della segnalazione – dimostrare che tali misure sono motivate da ragioni estranee alla segnalazione e non sono in nessun modo conseguenza della stessa. Sono altresì previste sanzioni pecuniarie amministrative elevate in tutti i casi in cui si configurino atti discriminatori nel confronti del dipendente.

In base alla legge, occorre assicurare l'assoluta segretezza dell'identità del denunciante. Non potrà, per nessun motivo, essere rivelata l'identità del dipendente che segnala atti discriminatori e, nell'ambito del procedimento penale, il segreto della segnalazione sarà garantita nei modi e nei termini di cui all'art. 329 del c.p.p. La segnalazione è sottratta all'accesso previsto dagli artt. 22 e seguenti della l. 7 agosto 1990, n. 241, e successive modificazioni.

Codice antimafia

La legge prevede che l'Anac, sentito il Garante, elabori le linee guida sulle procedure di presentazione e gestione delle segnalazioni promuovendo anche strumenti di crittografia quanto al contenuto della denuncia e alla relativa documentazione al fine di assicurare la riservatezza dell'identità del segnalante.

5) Legge 17 ottobre 2017, n. 161, recante modifiche al codice delle leggi antimafia e delle misure di prevenzione, di cui al d.lgs. 6 settembre 2011, n. 159, al codice penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale e altre disposizioni. Delega al Governo per la tutela del lavoro nelle aziende sequestrate e confiscate.

La nuova normativa punta a velocizzare le misure di prevenzione patrimoniale, a rendere più trasparente la scelta degli amministratori giudiziari, a ridisegnare l'Agenzia per i beni sequestrati ed include corrotti, *stalker* e terroristi tra i possibili destinatari dei citati provvedimenti. Si tratta del quarto provvedimento recante modifiche al codice delle leggi antimafia e delle misure di prevenzione, di cui al d.lgs. n. 159/2011.

In particolare, tra le disposizioni di maggiore interesse si segnalano quelle relative all'estensione dell'ambito di applicazione delle misure di prevenzione personali e patrimoniali agli indiziati dei reati di assistenza agli associati, truffa aggravata per il conseguimento di erogazioni pubbliche, terrorismo, *stalking* nonché di associazione per delinquere finalizzata ad alcuni gravi delitti contro la pubblica amministrazione, tra i quali, in particolare, il reato di corruzione, come pure quelle volte ad assicurare maggiore trasparenza e celerità al procedimento per l'applicazione delle misure di prevenzione, anche attraverso l'istituzione in sede distrettuale di sezioni o collegi giudicanti specializzati nonché a garantire la trattazione prioritaria del procedimento di prevenzione patrimoniale: viene infatti prevista una corsia preferenziale nella trattazione dei processi nei quali vi siano beni sequestrati.

Una delle novità principali della riforma del codice antimafia è contenuta nell'art. 33, che amplia le cause ostative all'assunzione dell'incarico di amministratore giudiziario, intervenendo direttamente sulle modalità di nomina dello stesso, attraverso la modifica dell'art. 7-*bis* dell'ordinamento giudiziario, di cui al r.d. 30 gennaio 1941, n. 12. In primo luogo, viene sancito che gli amministratori giudiziari dovranno essere scelti tra gli iscritti all'apposito albo secondo regole di trasparenza che assicurino la rotazione degli incarichi. Spetterà al Ministro della giustizia individuare criteri di nomina che, tra l'altro, tengano conto del numero degli incarichi in corso. Non potranno più assumere l'ufficio di amministratore giudiziario, il coadiutore o diretto collaboratore, il coniuge, i parenti e gli affini, i conviventi o i commensali abituali del magistrato che conferisce l'incarico.

A tali esclusioni ne sono state aggiunte delle altre, tra cui:

– la condanna a pene accessorie previste dalla legge fallimentare;

– l'essere stati rinviati a giudizio per i reati di cui all'art. 4 del codice delle leggi antimafia (soggetti destinatari delle misure di prevenzione personali);

– l'avere svolto attività lavorativa o professionale in favore del proposto o delle imprese allo stesso riconducibili;

– essere legati da uno "stabile rapporto di collaborazione professionale" con il coniuge o i figli del magistrato.

Legge di delegazione europea

6) Legge 25 ottobre 2017, n. 163, recante la delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017.

Fra gli articoli più rilevanti per gli aspetti di protezione dei dati personali si segnalano:

– l'art. 11, recante il criterio direttivo per l'attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla

protezione delle persone fisiche con riguardo 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, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;

– l'art. 12, che detta i princìpi e criteri direttivi per l'attuazione della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR);

– l'art. 13, che reca la delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, regolamento che viene a costituire lo strumento applicabile in via generale all'interno dell'Unione europea a tutti i trattamenti di dati svolti sia dal settore pubblico che in ambito privato.

La direttiva (UE) 2016/680, recepita con il decreto legislativo 18 maggio 2018, n. 51, è parte del cd. pacchetto protezione dati che, con il RGPD, definisce il quadro normativo europeo in materia di protezione dei dati personali. Si tratta del primo strumento cogente attraverso il quale si dettano principi armonizzati applicabili non solo alla comunicazione e scambio di dati personali tra le autorità di esecuzione della legge dei Paesi dell'Unione europea, ma a tutte le operazioni di trattamento di dati svolte dalle autorità pubbliche competenti a fini di prevenzione, contrasto e repressione dei reati nonché all'esecuzione delle pene.

La direttiva (UE) 2016/681, prevede l'obbligo dei vettori aerei di trasferire alle autorità nazionali di esecuzione della legge, competenti in base alla funzioni svolte, i dati relativi alle intenzioni di potenziali viaggiatori da e verso destinazioni internazionali, europee e, a scelta, nazionali per l'analisi dei possibili rischi, da svolgere attraverso la creazione di un'unità informazioni passeggeri (UIP) a ciò incaricata. La delega prevede che l'Italia si avvalga di tale opzione includendo i dati dei voli nazionali. La direttiva prevede alcune tutele in materia di protezione dei dati personali e in sede di attuazione dovrà rispettare i principi generali introdotti dalla direttiva (UE) 2016/680.

Si ritiene opportuno soffermare l'attenzione sul menzionato art. 13 della legge, attraverso il quale il Governo viene delegato ad adottare (entro il 21 maggio 2018) "uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679" mediante:

– abrogazione specifica ed espressa delle norme del Codice incompatibili con le nuove regole del regolamento;

– modifica e integrazione del Codice limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (cioè i casi di rinvio a più specifiche misure da prevedersi con norme nazionali);

– modifica del Codice, anche per quanto concerne il sistema sanzionatorio penale e amministrativo vigente, adeguandolo alle disposizioni del regolamento con previsione di sanzioni penali e amministrative "efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse";

– coordinamento delle disposizioni vigenti in materia di protezione dei dati personali contenute in altre leggi diverse dal Codice con le disposizioni del regolamento.

L'art. 13 precisa anche che il tutto potrà avvenire prevedendo altresì nei decreti delegati, "ove opportuno", il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante nell'ambito e per le finalità previste dal RGPD.

7) Legge 4 agosto 2017, n. 124, legge annuale per il mercato e la concorrenza.

L'art. 47, l. n. 99/2009, stabilisce che ogni anno il Governo, su proposta del

Mise, sentita la Conferenza unificata Stato-città-autonomie locali-regioni, tenendo conto anche delle segnalazioni eventualmente trasmesse dall'Autorità garante della concorrenza e del mercato, presenti alle Camere il disegno di legge annuale per il mercato e la concorrenza. La legge n. 124/2017 è ad oggi la prima legge annuale per il mercato e la concorrenza ed ha avuto un lungo e travagliato *iter* dalla sua presentazione risalente al 2015. Essa, intervenendo su molteplici settori di interesse dell'Autorità, contiene misure in materia di: assicurazioni, con particolare riguardo al campo della RC auto; comunicazioni; servizi postali; energia, banche, professioni nonché nell'ambito della distribuzione farmaceutica.

Assicurazioni

Con riferimento alle assicurazioni, la legge (art. 1, commi 2-40) reca molteplici norme di particolare interesse per l'Autorità.

Il comma 20, dell'art. 1, concernente disposizioni relative al valore probatorio dei dati acquisiti mediante le cd. scatole nere e altri dispositivi elettronici. Al riguardo, i dati sull'attività del veicolo devono essere gestiti in sicurezza dagli operatori del settore sulla base dello standard tecnologico comune che un decreto del Mise dovrebbe definire (ai sensi dell'art. 32, comma 1-*ter*, d.l. n. 1/2012) e sono successivamente inviati alle rispettive compagnie di assicurazione. Il decreto ministeriale deve essere adottato sentito il Garante al fine di definire lo standard tecnologico comune *hardware* e *software* per la raccolta, la gestione e l'utilizzo dei dati registrati dai meccanismi elettronici (scatole nere), al quale le imprese di assicurazione dovranno adeguarsi entro due anni dalla sua emanazione. Il decreto non è stato tuttavia ancora emanato, anche se il Mise ha dichiarato di averne notificato uno schema alla Commissione UE nel settembre 2012, ai sensi della direttiva 98/34/CE.

Ai sensi dell'art. 32, d.l. n. 1/2012, comma 1-*bis*, l'Ivass, di concerto con il Ministro dello sviluppo economico e il Garante, avrebbe dovuto stabilire, entro 90 giorni dall'entrata in vigore della legge di conversione del d.l. n. 1/2012, le modalità di raccolta, gestione e utilizzo, in particolare ai fini tariffari e della determinazione delle responsabilità in occasione dei sinistri, dei dati raccolti dalle scatole nere, nonché le modalità per assicurare la loro interoperabilità in caso di sottoscrizione da parte dell'assicurato di un contratto di assicurazione con impresa diversa da quella che ha provveduto ad installare tale meccanismo. In particolare si evidenzia che il Garante aveva già contribuito alla redazione di uno schema del suddetto regolamento, sottoposto a consultazione pubblica da parte dell'Ivass il 19 marzo 2013 (e che non risulta tuttavia ancora adottato).

Comunicazioni

Con riguardo al settore delle comunicazioni, la nuova legge sulla concorrenza prevede di eliminare una serie di vincoli che sono oggi presenti nei contratti con i fornitori di servizi di telefonia, televisivi e di comunicazioni elettroniche. In particolare viene previsto che:

– le spese di recesso e trasferimento dell'utenza siano note e commisurate al valore del contratto e ai costi reali sopportati dall'azienda, ovvero ai costi sostenuti per dismettere la linea telefonica o trasferire il servizio, e siano comunicati in via generale all'Agcom;

– le modalità di recesso siano semplici e analoghe a quelle di attivazione e sia garantito al cliente di comunicare il recesso o il cambio di gestore con modalità telematiche;

– nel caso di offerte promozionali aventi ad oggetto la fornitura sia di servizi che di beni, il contratto non possa avere durata superiore a ventiquattro mesi e la penale sia equa e proporzionata al valore del contratto;

– i gestori debbano avere il previo consenso espresso dai clienti per l'eventuale addebito del costo di servizi in abbonamento offerti da terzi; è fatto inoltre divieto

agli operatori di telefonia e di comunicazioni elettroniche di prevedere la possibilità per il consumatore o per l'utente di ricevere servizi in abbonamento da parte dello stesso operatore, o di terzi, senza il previo consenso espresso e documentato all'attivazione di tale tipologia di servizi.

Rilevante ricordare che, con riferimento al *telemarketing*, nel corso dei lavori parlamentari sul d.d.l. concorrenza si erano accolti taluni emendamenti di modifica dell'art. 130 del Codice – poi confluiti in un espresso comma – volti a prevedere la possibilità da parte degli operatori e dei soggetti terzi di stabilire, con chiamate vocali effettuate con addetti, un "primo" contatto anche non sollecitato con l'abbonato per fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, condizionando tale chiamata all'esplicito consenso del destinatario al proseguimento della conversazione (già in corso). Tale disposizione, ove introdotta nell'ordinamento, avrebbe comportato un rilevante pregiudizio per la protezione dei dati, la riservatezza e la tranquillità individuale dei destinatari delle telefonate con operatore in quanto avrebbe consentito la chiamata a contenuto promozionale in assenza del previo consenso dell'interessato. Infatti, la stessa chiamata diretta a richiedere il consenso, ha già di per sé natura promozionale. In altre parole, si stabiliva che l'operatore potesse chiamare chiunque e chiedere il consenso alla chiamata commerciale in diretta, senza tener conto del consenso preventivo dell'abbonato e della conferma implicita del diritto di prima chiamata. A seguito dell'intervento del Garante – nel quale è stato sottolineato che eliminare il requisito del consenso preventivo per le chiamate promozionali avrebbe di fatto liberalizzato il fenomeno del cd. *telemarketing* selvaggio (cfr. dichiarazione del Presidente del 4 maggio 2017, doc. web n. 6328158) – la menzionata disposizione è stata soppressa.

La legge istituisce, ai commi 44 e 45, il registro dei soggetti che utilizzano indirettamente risorse nazionali di numerazione, tenuto dall'Agcom. Con successivo decreto del Mise saranno determinati i criteri per l'individuazione dei soggetti da iscrivere nel registro.

Al fine di semplificare le procedure di migrazione tra operatori di telefonia mobile e quella per l'integrazione di Sim card aggiuntive o per la sostituzione di Sim card richieste da utenti già clienti di un operatore, con decreto del Ministro dell'interno, di concerto con il Mise, sono previste misure per l'identificazione in via indiretta del cliente, anche utilizzando il sistema pubblico dell'identità digitale (Spid) previsto dall'articolo 64 del Cad, in modo da consentire che la richiesta di migrazione e di integrazione di Sim card e tutte le operazioni ad essa connesse possano essere svolte per via telematica (comma 46).

Al fine di promuovere la massima diffusione dei pagamenti digitali ed elettronici, ivi inclusi i micropagamenti con credito telefonico per l'acquisto di biglietti per l'accesso a istituti e luoghi di cultura o per manifestazioni culturali, può farsi ricorso alla bigliettazione elettronica attraverso strumenti di pagamento in mobilità tramite qualsiasi dispositivo di telecomunicazione, anche attraverso l'addebito diretto su credito telefonico. Il titolo digitale del biglietto è consegnato sul dispositivo di comunicazione (comma 47).

Con riferimento inoltre al Registro pubblico delle opposizioni (Rpo), la legge prevede (al comma 54) che sia aggiornato il regolamento di istituzione e gestione del Registro delle opposizioni, cioè il registro pubblico degli abbonati che si oppongono all'utilizzo del proprio numero telefonico per vendite o promozioni commerciali, al fine di estendere la disciplina vigente – che si riferisce esclusivamente all'utilizzabilità per finalità commerciali della numerazione telefonica degli abbonati – anche alle ipotesi di impiego della posta cartacea per le medesime finalità. Al

riguardo il Garante ha reso il proprio parere rispetto allo schema di decreto del Presidente della Repubblica con il quale si è inteso dare attuazione all'articolo 130, comma 3-*bis*, del Codice, estendendo così la disciplina del Rpo all'impiego degli indirizzi presenti negli elenchi di cui all'art. 129, comma 1, del Codice, per l'invio di posta cartacea per le medesime finalità (provv. 29 dicembre 2017, n. 565, doc. web n. 7656748).

Tale regolamentazione andrà coordinata con le ulteriori modifiche regolamentari previste da un recente intervento normativo in materia, la legge 11 gennaio 2018, n. 5 (Nuove disposizioni in materia di iscrizione e funzionamento del registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato), con la quale si è, tra l'altro, estesa la possibilità di iscrizione nel Rpo delle numerazioni non presenti negli elenchi telefonici pubblici (art. 1, comma 2) e si è stabilito che l'iscrizione al Rpo comporta la revoca del consenso precedentemente espresso "con qualsiasi forma o mezzo e a qualsiasi soggetto", precludendo altresì, per le medesime finalità commerciali, "l'uso delle numerazioni telefoniche cedute a terzi dal titolare del trattamento sulla base dei consensi precedentemente rilasciati" (art. 1, comma 5). Tale disciplina sarà completamente operativa (con ulteriore aggiornamento, quindi, del d.P.R. n. 178/2010) a seguito dell'emanazione del regolamento attuativo previsto dall'art. 1, comma 15, l. n. 5/2018, in vista del quale il Mise ha istituito un tavolo tecnico ai cui lavori ha partecipato anche personale dell'Autorità.

Servizi postali

Con riguardo ai servizi postali è soppressa, a decorrere dal 10 settembre 2017, l'attribuzione in esclusiva alla società Poste italiane s.p.a. (quale fornitore del servizio postale universale) dei servizi inerenti le notificazioni e comunicazioni di atti giudiziari nonché dei servizi inerenti le notificazioni delle violazioni del codice della strada. Contestualmente si prevede che, entro novanta giorni dall'entrata in vigore della legge, l'Agcom determini, sentito il Ministro della giustizia, i requisiti e gli obblighi, nonché i requisiti di affidabilità, professionalità e onorabilità, per il rilascio delle licenze individuali relative alla notificazioni e comunicazioni di atti giudiziari e alle notificazioni delle violazioni del codice della strada (commi 57-58).

Energia

Con riguardo al settore dell'energia, la nuova legge determina la cessazione del regime di maggior tutela nel settore del gas naturale e nel settore dell'energia elettrica (comma 60).

Le modalità di superamento del regime della maggior tutela prevedono che entro sei mesi dall'entrata in vigore della legge l'Aeegsi trasmetta al Ministro per lo sviluppo economico il rapporto relativo al monitoraggio dei mercati di vendita al dettaglio dell'energia e del gas. Tra gli indicatori contenuti nel rapporto vi è anche la tutela delle famiglie in condizioni di disagio economico, nonché l'accrescimento del sistema di vigilanza e di informazione a tutela dei consumatori. Sulla base dei dati contenuti nel rapporto, il Mise adotta un decreto che dà conto del raggiungimento degli obiettivi e definisce le misure necessarie affinché la cessazione del regime della maggior tutela e l'ingresso consapevole nel mercato dei clienti finali avvenga secondo meccanismi che assicurino la concorrenza. A decorrere dal 1° gennaio 2018, i clienti finali di energia elettrica riforniti in maggior tutela devono ricevere adeguata informativa da parte di ciascun fornitore in relazione al superamento delle tutele di prezzo, secondo le modalità definite con provvedimento dell'Aeegsi.

A tutela del consumatore sono previste ulteriori diverse misure, tra le quali si segnalano di particolare interesse:

– le procedure finalizzate ad ottenere offerte di fornitura di energia elettrica e gas, e garantirne la confrontabilità, tramite la realizzazione e la gestione, da parte del

gestore del sistema informativo integrato, di un portale informatico per la raccolta e la pubblicazione delle offerte sul mercato *retail* e l'adozione da parte dell'Aeegsi, di linee guida per la promozione delle offerte commerciali di energia elettrica e gas a favore di gruppi di acquisto;

– l'erogazione ed eventuale rimodulazione del *bonus* elettrico e del *bonus* gas, ossia dei benefici economici a sostegno dei clienti economicamente svantaggiati e dei clienti domestici presso i quali sono presenti persone che versano in gravi condizioni di salute, tali da richiedere l'utilizzo di apparecchiature medico-terapeutiche, alimentate ad energia elettrica, necessarie per il loro mantenimento in vita (commi 75-77);

– le misure per la trasparenza del mercato dell'energia elettrica e del gas, tramite l'istituzione presso il Mise di un elenco dei soggetti abilitati alla vendita ai clienti finali (commi 80-84);

– le norme di promozione della concorrenza, attraverso la riduzione delle asimmetrie informative, anche intersettoriali, nel rispetto delle prescrizioni stabilite dal Garante (comma 85).

Trasporti

Con riguardo ai servizi di trasporto pubblico locale, la legge prevede in capo al concessionario l'obbligo di fornire un servizio di biglietteria telematica accessibile via internet attraverso un sito internet dedicato (comma 167) e, a tutela degli utenti dei servizi di trasporto di linea, l'obbligo per i concessionari ed i gestori di servizi di linea di trasporto passeggeri su gomma o rotaia e di trasporto marittimo di informare i passeggeri sulle modalità per accedere alla carta dei servizi, consentendo loro di prendere cognizione delle condizioni che danno titolo a fruire di rimborsi e indennizzi (comma 168).

Al fine di favorire l'offerta di servizi pubblici e privati per la mobilità, l'utilizzo di dati aperti, lo sviluppo delle *smart city*, nonché l'adozione di piani urbani della mobilità sostenibile, viene prevista una delega al Governo affinché adotti uno o più decreti legislativi diretti a disciplinare l'installazione sui mezzi di trasporto delle cd. scatole nere o altri dispositivi elettronici similari, volti anche a realizzare piattaforme tecnologiche per uno sviluppo urbano integrato multidisciplinare, nel rispetto e in coerenza con la normativa dell'Unione europea in materia. Ciò attraverso specifici decreti legislativi da adottarsi su proposta del Presidente del Consiglio dei ministri, di concerto con il Ministro delle infrastrutture e dei trasporti, sentiti l'Ivass e previo parere del Garante (comma 184).

Vaccini

8) Legge 31 luglio 2017, n. 119, conversione in legge, con modificazioni, del d.l. 7 giugno 2017, n. 73, recante disposizioni urgenti in materia di prevenzione vaccinale.

L'art. 1, d.l. 7 giugno 2017, n. 73, prevede che, al fine di assicurare la tutela della salute pubblica e il mantenimento di adeguate condizioni di sicurezza epidemiologica in termini di profilassi e di copertura vaccinale, "per i minori di età compresa tra zero e sedici anni e per tutti i minori stranieri non accompagnati sono obbligatorie e gratuite, in base alle specifiche indicazioni del calendario vaccinale nazionale relativo a ciascuna corte di nascita, le vaccinazioni di seguito indicate: a) anti-poliomielitica; b) anti-difterica; c) anti-tetanica; d) anti-epatite B; e) anti-pertosse; f) *anti-Haemophilus influenzae* tipo b" (art. 1, comma 1). Agli stessi fini, "sono altresì obbligatorie e gratuite, le vaccinazioni di seguito indicate: a) anti-morbillo; b) anti-rosolia; c) anti-parotite; d) anti-varicella" (art. 1, comma 1-*bis*)". Il medesimo decreto prevede anche i casi in cui le vaccinazioni possano essere omesse o differite.

Di particolare importanza risulta la disposizione secondo la quale devono essere previste, a decorrere dall'anno scolastico 2019/2020, misure di semplificazione per gli adempimenti vaccinali in funzione dell'iscrizione al sistema di istruzione, richie-

dendo ai dirigenti scolastici delle istituzioni del sistema nazionale di istruzione, ai responsabili dei servizi educativi per l'infanzia, dei centri di formazione professionale regionale e delle scuole private non parificate, la trasmissione alle aziende sanitarie locali territorialmente competenti, entro il 10 marzo, dell'elenco degli iscritti.

Le aziende sanitarie, effettuate le necessarie verifiche, devono provvedere a restituire i predetti elenchi alle scuole "con l'indicazione dei soggetti che risultano non in regola con gli obblighi vaccinali, che non ricadono nelle condizioni di esonero, omissione o differimento delle vaccinazioni in relazione a quanto previsto dall'art. 1, commi 2 e 3, e che non abbiano presentato formale richiesta di vaccinazione all'azienda sanitaria locale competente".

A seguito di tale acquisizione, i dirigenti scolastici e i responsabili dei servizi educativi per l'infanzia, dei centri di formazione professionale regionale e delle scuole private non parificate invitano i genitori, i tutori o i soggetti affidatari dei minori indicati negli elenchi a depositare "la documentazione comprovante l'effettuazione delle vaccinazioni ovvero l'esonero, l'omissione o il differimento delle stesse, in relazione a quanto previsto dall'art. 1, commi 2 e 3 o la presentazione della formale richiesta di vaccinazione all'azienda sanitaria locale territorialmente competente". La documentazione così prodotta o l'eventuale mancato deposito nel termine previsto saranno comunicati dalla scuola all'azienda sanitaria locale, per gli adempimenti previsti, anche di tipo sanzionatorio (art. 3-*bis*). La predetta procedura, descritta dall'art. 3-*bis*, d.l. n. 73/2017, è stata anticipata a decorrere dall'anno scolastico 2018/2019 e già per l'anno scolastico in corso, nelle sole regioni e province autonome presso le quali sono già istituite anagrafi vaccinali, nel rispetto delle modalità operative definite dal Ministero della salute e dal Ministero dell'istruzione sentito il Garante e a condizione che il controllo sul rispetto degli adempienti vaccinali si concluda entro e non oltre il 10 marzo 2018 (art. 18-*ter*, d.l. 16 ottobre 2017, n. 148).

Al fine di favorire il rispetto degli obblighi vaccinali nei termini previsti dalla legge, all'indomani della sua emanazione il Garante, facendo seguito alle numerose richieste delle amministrazioni pubbliche di poter effettuare uno scambio automatico di dati sulla regolarità vaccinale (previsto solo a partire dal 2019), ha adottato con procedura urgente – in considerazione dell'esigenza segnalata e dell'imminente avvio dell'anno scolastico – un provvedimento a valenza generale che autorizza una comunicazione di dati personali non sensibili dalle scuole alle autorità sanitarie (provv. 1° settembre 2017, doc. web n. 6765917). In base a tale provvedimento, gli istituti scolastici e i servizi educativi per l'infanzia hanno potuto trasmettere gli elenchi degli iscritti alle Asl competenti per territorio per consentire la verifica della regolarità vaccinale senza aggiungere oneri burocratici a famiglie e pubblica amministrazione (v. *amplius* par. 5.2.1).

Manovra correttiva di bilancio

9) Legge 21 giugno 2017, n. 96, conversione in legge, con modificazioni, del decreto-legge 24 aprile 2017, n. 50, recante disposizioni urgenti in materia finanziaria, iniziative a favore degli enti territoriali, ulteriori interventi per le zone colpite da eventi sismici e misure per lo sviluppo.

Tra le principali misure della legge in tema di entrate va segnalata l'introduzione (articolo 1-*bis*) della cd. web *tax*. A discapito della denominazione, non si tratta di una tassa per le imprese del web, ma di un procedimento di "cooperazione e collaborazione rafforzata" riservato a tutti i soggetti non residenti, indipendentemente dal tipo di attività esercitata e finalizzata alla definizione dei debiti tributari dell'eventuale stabile organizzazione presente nel territorio dello Stato. Possono accedervi le società non residenti che appartengono a gruppi multinazionali con ricavi al di sopra di una soglia predeterminata e che effettuano cessione di beni e prestazioni di servizio in Italia.

Vengono altresì disposti, agli artt. 5 e 6, incrementi della tassazione sui tabacchi e sui giochi e, con gli articoli 5-*bis* e 6-*bis*, si è previsto che l'Agenzia delle dogane e dei monopoli proceda all'inibizione dei siti web recanti offerta di taluni prodotti da tabacchi ovvero di pubblicità di giochi, scommesse e concorsi operanti in difetto di concessione o autorizzazione.

La legge fornisce una definizione di "locazione breve", prevedendo quali siano gli adempimenti connessi alla trasmissione dei dati a carico dei soggetti che esercitano attività di intermediazione immobiliare e che gestiscono portali telematici (art. 4, commi 4 e 6). Tali soggetti, mettendo in contatto persone che ricercano immobili con persone che dispongono di unità immobiliari da locare, devono trasmettere i dati relativi ai contratti conclusi loro tramite, entro il 30 giugno dell'anno successivo a quello a cui gli stessi si riferiscono. L'omessa, incompleta o infedele comunicazione dei dati relativi ai contratti è soggetta a sanzione (prevista all'art. 11, comma 1, d.lgs. n. 471/1997), ridotta alla metà se la trasmissione è effettuata entro i 15 giorni successivi alla scadenza, ovvero se, nel medesimo termine, è effettuata la corretta trasmissione dei dati.

Al fine di regolare le modalità di trasmissione e la conservazione dei suddetti dati da parte dell'intermediario, il legislatore ha previsto che, entro novanta giorni dall'entrata in vigore del decreto, vengano stabilite, con provvedimento del direttore dell'Agenzia delle entrate, senza prevedere alcun intervento o parere del Garante, le disposizioni di attuazione dei commi 4, 5 e 5-*bis* dell'art. 4.

Tra le disposizioni che incidono in tema di lavoro e previdenza possono segnalarsi quelle con cui si precisano meglio le caratteristiche di determinate attività lavorative ai fini della corresponsione della cd. Ape sociale (cfr. par. 4.8), nonché della applicazione della riduzione del requisito dell'anzianità contributiva in favore dei cd. lavoratori precoci.

In materia sanitaria vengono regolati i flussi informativi delle prestazioni farmaceutiche oltre che il trattamento dati del Nuovo sistema informativo sanitario – NSIS (artt. 29 e 32, comma 3). Tali disposizioni prevedono che: per monitorare ed accertare la spesa per l'assistenza farmaceutica ospedaliera, nel biennio 2016-2017, l'Aifa si avvalga dei dati di fatturato delle aziende farmaceutiche trasmessi attraverso il sistema di interscambio, introducendosi dal 2018 alcuni obblighi nell'ambito delle fatture elettroniche; per recepire quanto stabilito in sede di intesa Stato-regioni sulla riduzione delle risorse di edilizia sanitaria vengano modificate alcune regole di contabilizzazione da parte delle regioni nel 2018; il trasferimento dal Ministero dell'interno a quello della salute delle competenze relative al finanziamento delle prestazioni sanitarie urgenti od essenziali agli stranieri non in regola con le norme sul soggiorno.

Rilevanti inoltre le disposizioni che prevedono misure urgenti per la promozione della concorrenza e la lotta all'evasione tariffaria nel trasporto pubblico locale. In particolare si prevede che "le rilevazioni dei sistemi di videosorveglianza presenti a bordo dei veicoli e sulle banchine di fermata possono essere utilizzate ai fini del contrasto dell'evasione tariffaria e come mezzo di prova nel rispetto della normativa vigente in materia di trattamento dei dati personali, per l'identificazione di eventuali trasgressori che rifiutino di fornire le proprie generalità agli agenti accertatori, anche con eventuale trasmissione alle competenti forze dell'ordine".

Cyberbullismo

10) Legge 29 maggio 2017, n. 71, Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo.

All'esito di un ampio dibattito, cui pure ha preso parte il Garante (v. audizione del Presidente del Garante presso la Commissione giustizia e affari sociali, sulle proposte di legge in materia di prevenzione e contrasto del cyberbullismo, doc. web n. 4452702),

è stata infine adottata la l. 29 maggio 2017, n. 71, che, all'art. 1, contiene la definizione di cyberbullismo, condotta consistente in "qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti *online* aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

L'obiettivo della legge è quello di contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela ed educazione nei confronti dei minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti, assicurando l'attuazione degli interventi senza distinzione di età nell'ambito delle istituzioni scolastiche.

In base alle nuove disposizioni (art. 2), ciascun minore ultraquattordicenne vittima di cyberbullismo (ovvero i suoi genitori o chi esercita la responsabilità del minore) può inoltrare al titolare del trattamento o al gestore del sito internet o del *social media* un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante, che è chiamato a provvedere entro 48 ore (cfr. cap. 9).

Viene inoltre previsto il piano di azione integrato ovvero un tavolo tecnico con lo specifico obiettivo di proporre piani e successivi interventi per la prevenzione e il contrasto del cyberbullismo (art. 3) ed entro trenta giorni dalla data di entrata in vigore della legge il Miur è chiamato ad adottare delle linee di orientamento per la prevenzione e il contrasto del cyberbullismo nelle scuole, anche avvalendosi della collaborazione della Polizia postale e delle comunicazioni. Le linee guida vanno aggiornate ogni due anni. Ogni istituto scolastico è tenuto ad individuare fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile presenti sul territorio. Il dirigente scolastico che venga a conoscenza di atti di cyberbullismo informa tempestivamente i genitori dei minori coinvolti. I regolamenti scolastici dovranno prevedere esplicite sanzioni disciplinari, commisurate alla gravità degli atti compiuti.

Responsabilità degli esercenti le professioni sanitarie

11) Legge 8 marzo 2017, n. 24, disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie.

La legge disciplina i temi della sicurezza delle cure e del rischio sanitario, della responsabilità dell'esercente la professione sanitaria e della struttura sanitaria pubblica o privata, delle modalità e caratteristiche dei procedimenti giudiziari aventi ad oggetto la responsabilità sanitaria, nonché degli obblighi di assicurazione e dell'istituzione del fondo di garanzia per i soggetti danneggiati da responsabilità sanitaria. Fra i suoi obiettivi primari, vi è quello di ridurre il contenzioso (civile e penale) avente ad oggetto la responsabilità medica, al tempo stesso garantendo un più efficace sistema risarcitorio nei confronti del paziente.

La nuova disciplina anzitutto chiarisce all'art. 1 che la sicurezza delle cure è parte costitutiva del diritto alla salute, la quale assume così un vero e proprio valore costituzionale alla luce dell'art. 32 Cost.

Viene creata la figura del "Garante del diritto alla salute" (art. 2) – funzione che potrà essere affidata dalle regioni all'ufficio del difensore civico –, che potrà essere adito gratuitamente dai destinatari di prestazioni sanitarie per la segnalazione, anche anonima, di disfunzioni nel sistema dell'assistenza sanitaria e socio-sanitaria, ed agirà ove necessario a tutela dell'interessato.

Viene poi contemplata l'istituzione in ogni regione, senza nuovi o maggiori oneri per la finanza pubblica, del centro per la gestione del rischio sanitario e la sicurezza del paziente, cui è affidato il compito di raccogliere i dati regionali sui rischi ed eventi avversi nonché sul contenzioso e di trasmetterli annualmente all'osservatorio nazionale delle buone pratiche sulla sicurezza in sanità. Tale osservatorio, ricevuti i dati, individua idonee misure per la prevenzione e gestione del rischio sanitario e il monitoraggio delle buone pratiche per la sicurezza delle cure nonché per la formazione e l'aggiornamento del personale esercente le professioni sanitarie.

L'art. 4 della legge sottopone all'obbligo di trasparenza le prestazioni sanitarie erogate dalle strutture pubbliche e private nel rispetto della normativa in materia di protezione dei dati personali, obbligando la direzione sanitaria a fornire in tempi rapidi la documentazione sanitaria relativa al paziente. Viene infine previsto l'obbligo per le strutture sanitarie pubbliche e private di pubblicare sul proprio sito internet i dati relativi ai risarcimenti erogati nell'ultimo quinquennio.

Infine, la riforma introduce precisi obblighi assicurativi in capo alle strutture sanitarie ed agli esercenti la professione sanitaria. In particolare, è previsto l'obbligo di assicurazione per la responsabilità contrattuale (ex artt. 1218 e 1228 c.c.) verso terzi e verso i prestatori d'opera, a carico delle strutture sanitarie e sociosanitarie, pubbliche e private, anche per i danni cagionati dal personale a qualunque titolo operante presso le strutture medesime.

2.1.2. I decreti legislativi

Nel 2017 sono stati approvati numerosi decreti legislativi che hanno riflessi in materia di protezione dei dati personali, fra i quali si menzionano in particolare alcuni decreti attuativi di direttive dell'Unione europea oltre a quelli attuativi della l. 12 agosto 2016, n. 170, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2015, con la quale il Parlamento ha delegato il Governo ad intervenire in materia di prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo. La gran parte dei decreti, come illustrato *infra*, è stata sottoposta al Garante che ha espresso il proprio parere:

Modifiche al Cad

1) Decreto legislativo 13 dicembre 2017, n. 217, recante disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'art. 1 della l. 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.

Il decreto legislativo n. 217/2017 è l'ultimo degli interventi correttivi al testo del decreto legislativo n. 82/2005. Le nuove disposizioni si inseriscono nel più ampio contesto degli interventi di "semplificazione amministrativa" previsti dalla legge delega n. 124/2015 e si prefiggono di accelerare l'attuazione, a livello nazionale, dell'agenda digitale europea, in coerenza peraltro con le previsioni dell'art. 63, d.lgs. n. 179/2016. Le norme correttive mirano a definire un quadro normativo idoneo ad abilitare e supportare le azioni di attuazione dell'agenda digitale, dotando cittadini, imprese e amministrazioni di strumenti e servizi idonei a rendere effettivi i diritti di cittadinanza digitale che rappresentano il fulcro della legge delega e del già richiamato decreto legislativo n. 179/2016.

Pur esprimendo parere positivo al suddetto schema di decreto legislativo (provv. 26 ottobre 2017, n. 436, doc. web n. 7221785), il Garante ha tuttavia ritenuto opportuno porre l'accento su taluni rischi connessi al trattamento dei dati, anzitutto quello derivante dall'accesso indiscriminato ai dati relativi al "domicilio digitale". Rendere pubblici tali elenchi, peraltro in formato aperto e senza specificare quali

dati personali contengano, comporta il rischio di favorire l'invio di *spam* e di aumentare considerevolmente i furti di identità. Il domicilio digitale dovrebbe invece essere utilizzabile solo per l'invio di comunicazioni avente valore legale o connesse al conseguimento di finalità istituzionali.

Il Garante ha inoltre ritenuto opportuno suggerire l'introduzione di maggiori tutele nella (obbligatoria) diffusione *online*, da parte del difensore civico digitale, delle segnalazioni ricevute dai cittadini concernenti la violazione della normativa sulla digitalizzazione della p.a. Tale obbligo, ad avviso del Garante, non solo comporta una diffusione sproporzionata di dati riferibili al segnalante, ma rischia di trasformarsi in un deterrente all'esercizio di tale diritto. Si auspica, quindi, che venga previsto sempre l'oscuramento dei dati personali eventualmente presenti nei documenti oggetto di pubblicazione *online*, sia nel caso di segnalazioni, sia nel caso di decisioni sulle stesse.

Il Garante è intervenuto anche in materia di accesso ai servizi digitali delle pp.aa. Con riferimento all'utilizzo dei dati anagrafici ha rilevato alcune criticità in merito alla loro protezione e, riaffermando principi già enunciati in precedenti pareri, ha ritenuto opportuna la previsione di maggiori tutele per il riserbo dei dati contenuti nelle "basi dati di interesse nazionale", osservando che, ai fini di una maggiore tutela, l'accesso ai servizi della p.a. in rete debba avvenire non solo in via esclusiva tramite Spid, ma anche attraverso l'utilizzo di altri sistemi (già disponibili), quali la carta di identità elettronica o la carta nazionale dei servizi.

All'indomani della pubblicazione del decreto legislativo è stato riscontrato l'inserimento nel testo di una disposizione, assente nello schema di decreto sottoposto all'attenzione del Garante in sede di parere, in grado di pregiudicare l'assetto delle garanzie sino ad allora assicurate nel trattamento dei dati personali nella p.a. Al riguardo, con una nota del Presidente del 22 gennaio 2018 (doc. web n. 8456134) l'Autorità, nel rimarcare la gravità della mancanza di un interpello preventivo del Garante su tale materia, ha dichiarato che l'introduzione del nuovo art. 50-*ter* del Cad – che ha istituito la piattaforma digitale nazionale dati, affidata in via sperimentale al Commissario straordinario per l'attuazione dell'Agenda digitale, laddove riferita ai dati personali – "fa sorgere diversi interrogativi in ordine alla compatibilità con la normativa europea sulla protezione dei dati". La creazione della suddetta piattaforma, porterebbe ad un accentramento e duplicazione di tutti i dati detenuti dalle pubbliche amministrazioni per finalità del tutto generiche, realizzando di fatto una concentrazione presso un unico soggetto di informazioni, anche sensibili e sensibilissime, con evidenti rischi di usi distorti e accessi non autorizzati (in merito v. pure par. 4.2).

Licenziamento disciplinare

2) Decreto legislativo 20 luglio 2017, n. 118, recante disposizioni integrative e correttive al d.lgs. 20 giugno 2016, n. 116, recante modifiche all'art. 55-*quater* del d.lgs. 30 marzo 2001, n. 165, ai sensi dell'art. 17, comma 1, lettera *s*), della l. 7 agosto 2015, n. 124, in materia di licenziamento disciplinare.

Il decreto, correttivo del precedente d.lgs. 20 giugno 2016, n. 116, ha introdotto modifiche alla disciplina del licenziamento disciplinare, prevista dall'art. 55-*quater*, d.lgs. 30 marzo 2001, n. 165, volte a rafforzare detto istituto al fine di un più efficace contrasto all'assenteismo nella p.a. In particolare, le disposizioni prevedono che nel caso in cui un pubblico dipendente attesti falsamente la propria presenza in servizio e tale assenza sia accertata in flagranza ovvero mediante strumenti di sorveglianza o di registrazione degli accessi o delle presenze, possa disporsi l'immediata sospensione cautelare senza stipendio del dipendente senza obbligo di preventiva audizione dello stesso (3-*bis*).

Il nuovo decreto ha poi apportato modifiche all'art. 1, d.lgs. n. 116/2016 prevedendo un termine più ampio per la denuncia al pubblico ministero e la segnalazione

alla competente procura regionale della Corte dei conti, che passa da 15 a 20 giorni, e per l'eventuale successiva azione di responsabilità che dovrà essere esercitata entro 150 (anziché 120) giorni successivi alla denuncia, senza possibilità di proroga.

È stato inoltre introdotto l'obbligo di comunicazione all'Ispettorato per la Funzione pubblica dei provvedimenti di cui ai commi 3-*bis* (provvedimento di sospensione cautelare dal servizio) e 3-*ter* (provvedimento di contestazione dell'addebito e di convocazione del dipendente dinanzi all'Ufficio procedimenti disciplinari e quelli conclusivi dei procedimenti), ai sensi di quanto previsto dall'articolo 55-*bis*, comma 4 (art. 3).

3) Decreto legislativo 25 maggio 2017, n. 90, recante l'attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006.

Il decreto legislativo adottato ai sensi della legge 12 agosto 2016, n. 170, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – legge di delegazione europea 2015, introduce significative modifiche alla vigente disciplina in materia di prevenzione dell'uso del sistema finanziario a fini di riciclaggio e di finanziamento del terrorismo allo scopo di allineare la normativa nazionale alle più recenti disposizioni introdotte in materia con la direttiva del Parlamento europeo e del Consiglio del 20 maggio 2015, (UE) 2015/849 (la quarta del settore), che integra ed abroga le direttive 2005/60/CE e 2006/70/CE e applica le raccomandazioni del Gruppo d'azione finanziario internazionale (Gafi). La direttiva intende operare un più rigoroso contrasto alla crescente diversificazione del mercato criminale, atteso che i flussi di denaro illecito, compromettendo la stabilità e l'integrità del settore finanziario, rappresentano una concreta minaccia per il mercato interno dell'Unione e dei singoli Stati membri. Considerata la dimensione e la pericolosità del riciclaggio e del finanziamento del terrorismo, facilitati dalla continua evoluzione della tecnologia e dei mezzi a disposizione dei criminali, l'adozione di misure di contrasto che consentano di adeguare il sistema di prevenzione a nuove ipotesi di riciclaggio è vista come imprescindibile.

Con provvedimento 9 marzo 2017, n. 125 (doc. web n. 6124534), il Garante ha espresso parere favorevole sullo schema di decreto legislativo, ancorché condizionato ad talune specifiche modifiche ed integrazioni. Ritenendo che lo scambio di informazioni tra Autorità di vigilanza e Guardia di finanza all'interno del Paese, come pure con le omologhe Istituzioni degli altri Paesi, costituisse un momento di elevato rischio, il Garante ha chiesto che venissero individuate misure idonee a garantire la protezione dei dati personali nelle comunicazioni dei dati da parte degli operatori finanziari all'Uif oltre che nella tenuta degli stessi e negli accessi alla banca dati.

Con riferimento alla consultazione dell'archivio Scipafi, è stata inoltre richiesta la previsione di una nuova disposizione che rinvii ad un decreto modificativo della disciplina attuale di accesso al sistema Scipafi prevista in particolare dal d.m. 19 maggio 2014, n. 95, che, previo parere del Garante, miri a specificare i presupposti, le categorie di soggetti che vi possono accedere, le procedure di abilitazione dei soggetti obbligati e i dati oggetto di riscontro per la verifica della veridicità dei dati forniti; tale suggerimento non è stato accolto.

Per assicurare il rispetto del principio di conservazione dei dati per il tempo strettamente necessario al raggiungimento delle finalità, in linea con quanto già affermato dall'Autorità, il Garante ha ritenuto necessaria un'attenta rivalutazione sulla effettiva congruità del periodo di almeno dieci anni per il quale è previsto che la Uif

conservi in "evidenza" le segnalazioni ritenute infondate, tenuto conto anche del fatto che si tratterebbe di informazioni già valutate come non rilevanti ai fini del contrasto del riciclaggio. Tale termine, infatti, è da ritenersi eccessivamente lungo e non in linea con le indicazioni comunitarie, che prevedono un termine non inferiore a 5 anni. Neanche tale osservazione risulta essere stata accolta dal legislatore.

4) Decreto legislativo 25 maggio 2017, n. 92, disposizioni per l'esercizio dell'attività di compro oro, in attuazione dell'art. 15, comma 2, lett. *l*), l. 12 agosto 2016, n. 170.

Il decreto legislativo n. 92/2017 detta disposizioni specifiche per la regolamentazione del commercio al dettaglio e all'ingrosso di oro, sul presupposto dell'elevata esposizione del settore al rischio di riciclaggio di denaro e reimpiego di beni di provenienza illecita. In esso viene previsto che l'esercizio dell'attività di compro oro sia riservato agli operatori (persone fisiche o società) iscritti nell'apposito ed istituendo registro tenuto dall'Oam (Organismo degli agenti in attività finanziaria e dei mediatori creditizi). L'iscrizione nel predetto registro, con l'attribuzione di un codice identificativo unico che riporta gli estremi dei documenti comunicati, avviene a seguito di verifica da parte dell'Oam della documentazione inviata; la mancata iscrizione nel medesimo registro costituisce esercizio abusivo dell'attività, sanzionata penalmente. Variazioni successive all'iscrizione dovranno essere comunicate al medesimo organismo; in difetto l'operatore incorrerà in sanzioni pecuniarie.

Prima del compimento di ogni operazione, gli esercenti di detta attività devono altresì provvedere all'identificazione del cliente, verificandone l'identità. L'assolvimento di quest'obbligo potrà avvenire, anche in caso di assenza dell'interessato, solo nel caso di clienti i cui dati risultino da atti pubblici, da scritture private autenticate o da certificati qualificati, o siano in possesso di un'identità digitale o di un certificato per la generazione di firma digitale, ovvero siano già stati identificati in relazione ad un altro rapporto o prestazione professionale in corso o, ancora, siano stati identificati attraverso forme e modalità individuate dall'Autorità di vigilanza di settore, tenendo conto delle tecniche di identificazione a distanza. Ogni operazione dovrà essere annotata su una scheda che indichi tutti i dati anagrafici del cliente, gli estremi dell'operazione e gli strumenti di pagamento.

Gli operatori sono tenuti alla conservazione per dieci anni, nel rispetto della normativa di protezione dei dati personali, dei dati relativi all'identificazione della clientela, della scheda predisposta e della copia della ricevuta consegnata. Questa documentazione, inoltre, dovrà essere accessibile da parte delle autorità competenti.

Il controllo sull'osservanza delle disposizioni previste dal decreto spetta alla Guardia di finanza; ogni operatore è tenuto a segnalare all'Unità di informazione finanziaria (Uif) eventuali operazioni sospette, secondo le disposizioni del decreto antiriciclaggio.

Il Garante, con provvedimento 9 marzo 2017, n. 126 (doc. web n. 6285103), ha espresso parere favorevole sullo schema di decreto legislativo, condizionato ad alcune modifiche. In particolare, con riferimento all'art. 3 dello schema di decreto, è stata rappresentata l'opportunità che nel richiamato successivo decreto ministeriale (che il Mef dovrà adottare entro tre mesi dall'entrata in vigore del decreto in parola), teso a stabilire le modalità tecniche di invio dei dati e di alimentazione del registro, venga acquisito il parere del Garante. In tale ottica, fermo restando l'obbligo di fornire l'informativa di cui all'art. 13 del Codice, si raccomanda di assicurare "il rispetto delle norme dettate dal codice in materia di protezione dei dati personali nonché il trattamento dei medesimi esclusivamente per le finalità di cui al presente decreto" sin dalla fase di istituzione del medesimo registro (principio *data protection by design* previsto all'art. 25, RGPD).

3 I rapporti con il Parlamento e le altre Istituzioni

3.1. *Le audizioni del Garante in Parlamento*

Nel 2017 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 del Presidente, tenutasi il 25 luglio 2017, presso il Comitato parlamentare per la sicurezza della Repubblica (Copasir), sul tema sicurezza e *privacy*;

b) un'audizione informale del Presidente dell'11 aprile 2017 presso la 8ª Commissione permanente (lavori pubblici, comunicazioni) del Senato della Repubblica, nell'ambito dell'esame del d.d.l. n. 2553 (attivazione del servizio *safety check*) e del d.d.l. n. 2575 (delega per tracciabilità autori di contenuti nelle reti sociali) (doc. web n. 6235402);

c) un'audizione del Presidente presso le Commissioni riunite affari costituzionali e difesa della Camera dei deputati, sulle problematiche legate alla difesa e alla sicurezza nello spazio cibernetico il 7 marzo 2017 (doc. web n. 6059229).

3.2. *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 controllo del Parlamento riguardanti aspetti di specifico interesse in materia di protezione dei dati personali.

In particolare si segnala l'intervento dell'Autorità relativamente ad un atto di sindacato ispettivo, concernente il ripristino dell'obbligo di pubblicità dei dati relativi ai beneficiari dei finanziamenti provenienti dal Fondo europeo di garanzia (Feaga) e dal Fondo europeo agricolo di sviluppo regionale (Feasr). In tale occasione sono state fornite specifiche osservazioni alla Presidenza del Consiglio, precisando che rispetto agli oneri di pubblicazione relativi all'erogazione dei fondi agricoli europei, sono previste specifiche regole di pubblicazione (e limiti alla stessa) per finalità di trasparenza direttamente nella disciplina di settore dell'Unione europea (cfr. art. 111 ss., regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio del 17 dicembre 2013 sul finanziamento, sulla gestione e sul monitoraggio della politica agricola comune e che abroga i regolamenti del Consiglio (CEE) 352/78, (CE) 165/94, (CE) 2799/98, (CE) 814/2000, (CE) 1290/2005 e (CE) 485/2008) non trovando applicazione altra disciplina generale in materia di trasparenza a carattere nazionale. Con riferimento ad alcuni ordini del giorno accolti che impegnavano il Governo a valutare l'opportunità di rivolgersi al Garante ai sensi dell'art. 154, comma 4, del Codice "al fine di acquisire ogni elemento di valutazione per fare quanto di propria competenza per la protezione dei dati personali" (nn. 9/3767/1, 9/3944/2, 9/1460-B/7, tutti presentati dall'on. Marzano), con nota 16 marzo 2017 è stato rappresentato alla Presidenza del

Consiglio dei ministri di non aver ricevuto alcuna richiesta di parere nei sensi indicati dai suddetti.

In particolare, si fa riferimento ad ordini del giorno collegati ai seguenti provvedimenti:

a) d.d.l. concernente la ratifica ed esecuzione dell'accordo sulla cooperazione di polizia e doganale tra il Governo della Repubblica italiana e il Consiglio federale svizzero, fatto a Roma il 14 ottobre 2013 (l. 28 luglio 2016, n. 155);

b) d.d.l. concernente la ratifica ed esecuzione dell'accordo di partenariato e cooperazione tra l'Unione europea e i suoi stati membri, da una parte, e la Repubblica dell'Iraq, dall'altra […], fatto a Bruxelles l'11 maggio 2012 nonché dell'accordo quadro di partenariato e cooperazione tra l'Unione europea e i suoi stati membri, da una parte, e la Repubblica delle Filippine, dall'altra, fatto a Phnom Penh, l'11 luglio 2012 (l. 3 ottobre 2016, n. 186).

c) d.d.l. concernente la ratifica ed esecuzione della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea, fatta a Bruxelles il 29 maggio 2000. Il disegno di legge, divenuto la l. 21 luglio 2016, n. 149, è in vigore dal 5 agosto 2016 e prevede che il Governo entro sei mesi dall'entrata in vigore adotti i necessari decreti legislativi attuativi. Con d.lgs. 5 aprile 2017, n. 52, sono state definite tali norme di attuazione e non risulta che al riguardo sia stato chiesto il parere dell'Autorità.

Sono state inoltre predisposte e inoltrate note informative ai Dipartimenti interessati, riguardanti:

1) l'interrogazione n. 3-04003, dell'on Taverna, concernente il trattamento dei dati relativi alle vaccinazioni da parte dei soggetti pubblici;

2) le interrogazioni nn. 5-03469, 5-07239 e 5-10594, 5-10907, dell'on Tancredi ed altri, relative ai provvedimenti presi dal Garante nell'arco di quattro anni nei confronti del Tribunale militare di Verona;

3) l'interrogazione a risposta scritta n. 4-18434 dell'on. Fantinati, concernente la tecnica del cd. *dynamic pricing*;

4) l'interrogazione a risposta scritta n. 4/08476 della Sen. De Pin, concernente la presunta cessione dati sanitari alla multinazionale Ibm;

5) l'informativa sull'interrogazione n. 5-11997 dell'on. Turco ed altri, in materia di accesso.

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

3.3.1. 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 provvedimento, di seguito riportati:

1) decreto del Ministero della giustizia per l'attuazione dell'art. 12, d.lgs. 12 maggio 2016 recante le regole procedurali di carattere tecnico-operativo relative agli scambi tra i casellari giudiziali europei (parere 12 gennaio 2017, n. 1, doc. web n. 6033692);

2) provvedimenti del Direttore dell'Agenzia delle entrate di modifica delle specifiche tecniche di comunicazione all'Anagrafe tributaria dei dati relativi ai contratti assicurativi, ai premi assicurativi, agli interessi passivi per contratti di mutuo, alle spese sanitarie rimborsate, alle spese universitarie e ai contributi versati alle forme pensionistiche complementari (parere 19 gennaio 2017, n. 11, doc. web n. 6064866);

3) provvedimenti del Direttore dell'Agenzia delle entrate inerenti le modalità tecniche di comunicazione all'Anagrafe tributaria, a decorrere dall'anno 2016, dei dati relativi ai rimborsi delle spese universitarie e dei dati relativi agli interventi di recupero del patrimonio edilizio e di riqualificazione energetica (parere 19 gennaio 2017, n. 12, doc. web n. 6064930);

4) provvedimento del Dipartimento generale italiani all'estero e le politiche migratorie concernente le specifiche tecniche di sicurezza del processo di emissione del passaporto elettronico (parere 26 gennaio 2017, n. 28, doc. web n. 5953053);

5) decreto del Ministro dell'interno recante attuazione dell'art. 53 del Codice in materia di protezione dati personali (parere 23 febbraio 2017, n. 74, doc. web n. 6197012);

6) d.P.R. per l'individuazione delle modalità di applicazione del Codice della *privacy* in attuazione dell'art. 57 ai trattamenti di dati personali per finalità di polizia effettuato da organi, uffici e comandi delle Forze di polizia (2 marzo 2017, n. 86, doc. web n. 6197365);

7) decreto del Ministero dell'interno recante disposizioni di attuazione all'art. 29, d.P.R. 7 aprile 2016, n. 87, regolamento recante disposizioni di attuazione della legge 30 giugno 2009, n. 85 concernente l'istituzione della banca dati del Dna (parere 9 marzo 2017, n. 127, doc. web n. 6163803);

8) regolamento del Ministero della salute relativo al Sistema informativo trapianti (Sit) (parere 30 marzo 2017, n. 164, doc. web n. 6407524)

9) provvedimento del Direttore dell'Agenzia delle entrate recante disposizioni attuative del decreto del Ministero dell'economia e delle finanze del 28 dicembre 2015 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 per quanto riguarda lo scambio automatico obbligatorio di informazioni nel settore fiscale. Modalità e termini di comunicazione delle informazioni (parere 22 giugno 2017, n. 283, doc. web n. 6587145);

10) documento tecnico del Mef sulle modalità di accesso ai dati di spesa sanitaria (5 luglio 2017, n. 300, doc. web n. 6843865);

11) decreto del Miur, applicativo del d.lgs. n. 76/2005 in materia di Anagrafe nazionale degli studenti (Ans) (parere 5 luglio 2017, n. 301, doc. web n. 6843964);

12) d.P.C.M. recante norme attuative delle disposizioni in materia di anticipo finanziario a garanzia pensionistica (Ape) (parere 26 luglio 2017, n. 335, doc. web n. 6820552);

13) d.P.C.M. recante modifiche al regolamento che disciplina le modalità di attribuzione ed utilizzo della carta elettronica, 18App (parere 26 luglio 2017, n. 336, doc. web n. 6821795);

14) decreto Ministero dell'interno, concernente l'individuazione delle modalità di applicazione del Codice *privacy* ai trattamenti effettuati dal centro elaborazione dati di cui all'art. 8, l. n. 121/1981 (parere 26 luglio 2017, n. 337, doc. web n. 6826534);

15) decreto del Mef di concerto con il Ministero della salute, concernente le modalità tecniche e i servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (Fse) di cui all'art. 12, comma 15-*ter*, d.l. 18 ottobre 2012, n. 179, come modificato dall'art. 1, comma 382, l. 11 dicembre 2016, n. 232 (parere 26 luglio 2017, n. 339, doc. web n. 6930323);

16) d.P.R. concernente regolamento recante norme per l'attuazione del sistema telematico centrale della nautica da diporto da emanarsi in attuazione dell'art. 1, comma 219, l. 24 dicembre 2012 (parere del 26 luglio 2017, n. 340, doc. web n. 6820644);

17) decreto del Ministero della salute recante la definizione del materiale informativo-educativo destinato ai donatori di sangue in relazione al rischio di trasmissione dell'infezione da HIV e del questionario per la raccolta delle informazioni post-donazione (parere 9 novembre 2017, n. 461, doc. web n. 7458918);

18) decreto del Mef, attuativo dell'art. 29, comma 2, d.l. 24 aprile 2017, n. 50, convertito dalla l. 21 giugno 2017, n. 96, recante disposizioni in materia di fatture elettroniche per acquisti di prodotti farmaceutici (parere 7 dicembre 2017, n. 516, doc. web n. 7457312);

19) d.P.R. recante modifiche al regolamento di cui al d.P.R. 7 settembre 2010, n. 178 ai sensi dell'art. 1, comma 54, l. 4 agosto 2017, n. 124 (Legge annuale per il mercato e la concorrenza, in materia di Registro pubblico delle opposizioni) (parere 29 dicembre 2017, n. 565, doc. web n. 7656748).

I pareri sugli schemi di provvedimento di cui ai punti 5), 6) e 14), hanno rivestito particolare importanza in quanto con la successiva attuazione dei provvedimenti stessi si dà compiuta attuazione alle prescrizioni del Codice per quanto attiene ai trattamenti di dati da parte delle Forze di polizia. Il decreto 24 maggio 2017, attuativo dell'art. 53 del Codice, contiene l'individuazione, nell'All. C del Codice, dei trattamenti di dati non occasionali ed dei relativi titolari (64 schede).

3.3.2. I pareri su norme di rango primario

L'Autorità è stata coinvolta dalla Presidenza del Consiglio dei ministri nell'adozione di alcuni atti normativi di rango primario, con la richiesta formale di parere su due schemi di decreto legislativo volti ad attuare la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (cfr. par. 2.1.2, punti 2 e 3). In particolare:

a) il primo schema su cui il Garante ha fornito parere prevedeva l'attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, recante la modifica delle direttive 2005/60/CE e 2006/70/CE e l'attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006 (parere 9 marzo 2017, n. 125, doc. web n. 6124534). Il suddetto schema è divenuto poi il d.lgs. 25 maggio 2017, n. 90 (cfr. par. 2.2.2, punto 2);

b) il secondo schema di decreto, invece, ha riguardato in particolare l'attuazione della direttiva (UE) 2015/849 (art. 2, par. 7), nella parte in cui reca disposizioni specifiche per la regolamentazione delle attività di compravendita di oro e oggetti preziosi usati (cd. compro oro), in attuazione dell'art. 15, comma 2, lettera *l*), l. 12 agosto 2016, n. 170 (parere 9 marzo 2017, n. 126, doc. web n. 6285103). Come già visto, tali disposizioni sono confluite nel d.lgs. 25 maggio 2017, n. 92, disposizioni per l'esercizio dell'attività di compro oro, in attuazione dell'art. 15, comma 2, lett. *l*), l. 12 agosto 2016, n. 170 (legge di delegazione europea per il 2015) (cfr. par. 2.2.2, punto 3).

È stato inoltre richiesto il parere del Garante sullo schema di decreto legislativo recante la revisione ed integrazione del decreto legislativo 18 luglio 2005, n. 171, recante codice della nautica da diporto e attuazione della direttiva 200/44/CE (parere 19 ottobre 2017, n. 420, doc. web n. 7273618).

Infine, nel mese di novembre 2017, è stato richiesto parere formale sullo schema di decreto legislativo recante disposizioni in materia di intercettazione di conversazioni o comunicazioni (parere 2 novembre 2017, n. 456, doc. web n. 7083069).

In termini più generali, occorre considerare che l'art. 154, comma 4, del Codice fa riferimento alla normativa avente rango secondario, anche se la correlata disposi-

zione della direttiva europea non reca una distinzione al riguardo (art. 28, par. 2). Le richieste di parere su atti primari si inquadrano oggi in un contesto di collaborazione con le amministrazioni interessate che l'Autorità, come più volte segnalato alla Presidenza del Consiglio, auspica possa ulteriormente svilupparsi, nella consapevolezza che sia di grande utilità il coinvolgimento del Garante nella fase preparatoria di iniziative legislative del Governo, oltre che regolamentari, al fine di valutarne previamente l'impatto sulla protezione dei dati personali e sui diritti delle persone. Ciò anche alla luce di quanto previsto dal nuovo pacchetto protezione dati adottato dall'Unione europea, ed in particolare dall'art. 36, par. 4, RGPD e dall'art. 28, par. 2, della direttiva 680/2016, che prevedono la consultazione obbligatoria del Garante anche durante l'elaborazione di proposte di atti legislativi.

3.4. *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 dettato costituzionale (art. 117, comma 2, lett. *l*), Cost.).

L'Autorità ha esaminato nel corso dell'anno otto leggi regionali, riscontrando per due di esse un corretto svolgimento della potestà legislativa regionale in relazione agli aspetti di protezione dei dati personali; si è trattato in particolare della legge Regione Friuli Venezia Giulia 9 dicembre 2016, n. 18, recante disposizioni in materia di sistema integrato del pubblico impiego regionale e locale e della legge Regione Campania 31 marzo 2017, n. 10, recante misure per l'efficientamento dell'azione amministrativa e l'attuazione degli obiettivi fissati nel Derf 2017 – Collegato alla stabilità regionale per il 2017.

Negli altri casi, rilevati profili di criticità, sono state formulate osservazioni per lo più incentrate sulla ricorrente problematica delle implicazioni derivanti da iniziative legislative regionali tese a introdurre obblighi di diffusione di dati personali nuovi e/o ulteriori rispetto a quelli già previsti dalla normativa statale in materia di trasparenza.

L'Autorità ha così ritenuto necessario inoltrare alla Presidenza del Consiglio dei ministri alcune osservazioni in merito alla legge Regione Lazio 31 dicembre 2016, n. 17, recante la legge di stabilità regionale 2017, circa il nuovo regime di pubblicità/diffusione di dati personali dei soggetti che hanno fatto domanda per ottenere un beneficio economico, non essendo quest'ultimo previsto dalla normativa statale in materia di trasparenza (nota 7 febbraio 2017).

In merito alla legge Regione Friuli Venezia Giulia 9 maggio 2017, n. 13, recante disposizioni per le persone affette da fibromialgia, l'Autorità ha sottolineato l'assenza nella legge regionale del riferimento ai presupposti e principi previsti dalla normativa in materia di protezione dei dati, in particolare alle finalità di rilevante interesse pubblico perseguite nel trattamento dei dati contenuti nel registro regionale delle fibromialgie (nota 16 giugno 2017).

Rispetto alle ulteriori quattro leggi regionali il Garante ha ritenuto necessario fornire proprie osservazioni, aventi ad oggetto profili del testo non conformi con la normativa rilevante in materia di protezione dei dati personali e suscettibili di integrare, ancora una volta, un contrasto con gli artt. 3 e 117 della Costituzione.

Si è trattato della legge Regione Emilia-Romagna 1° giugno 2017, n. 9, recante

fusione dell'Ausl Reggio Emilia e dell'Azienda Arcispedale Santa Maria Nuova e altre disposizioni di adeguamento degli assetti organizzativi in materia sanitaria, sulla quale l'Autorità ha fornito le proprie osservazioni soffermandosi, in particolare, sugli obblighi di pubblicità previsti nella legge in questione che potrebbero configurare una invasione in una materia di esclusiva competenza dello Stato (nota 7 luglio 2017).

Sulla legge Regione Molise 6 ottobre 2017, n. 14, recante istituzione dei registri di patologie di rilevante interesse sanitario e di particolare complessità, l'Autorità ha inviato le proprie osservazioni, sottolineando la mancanza di un richiamo espresso ai principi descritti negli artt. 11 e 22 del Codice e alle autorizzazioni generali in relazione al trattamento dei dati sensibili contenuti nei registri di patologie (3 novembre 2017).

In relazione alla legge Regione Toscana 5 giugno 2017, n. 26, recante disposizioni in materia di diritto di accesso, di pubblicità e trasparenza per i consiglieri regionali, assessori e organi di garanzia, l'Autorità, come già avvenuto in precedenza per altre leggi regionali, ha rilevato l'introduzione di alcuni adempimenti in materia di trasparenza, quali obblighi di comunicazione e di pubblicità sul sito web istituzionale, e che alcuni di questi non siano previsti dalla normativa statale di settore mentre altri si sovrappongano ad essa (nota 10 luglio 2017).

Con l'ultima legge regionale presa in esame, legge Regione Umbria 24 novembre 2017, n. 17, si è ripresentato il possibile conflitto tra gli adempimenti in materia di pubblicità e trasparenza, tramite pubblicazione sul Bollettino ufficiale e sui siti web istituzionali della Regione di dati, informazioni e documenti per i quali non esiste un obbligo di pubblicazione. Posto che il diritto alla riservatezza e alla protezione dei dati personali devono essere ugualmente garantiti su tutto il territorio nazionale al fine di evitare disparità di trattamento (art. 3, Cost.), si è sottolineato ogni volta come gli interventi normativi delle regioni debbano essere compatibili con i pertinenti parametri costituzionali, a maggior ragione quando le iniziative legislative regionali introducano nuovi e ulteriori obblighi di diffusione di dati personali (cfr. Corte cost. 7 luglio 2005, n. 271).

L’attività svolta dal Garante

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*

Anche nel 2017 sono pervenute richieste di parere su schemi di regolamento per il trattamento di dati sensibili o giudiziari effettuati dalle amministrazioni pubbliche.

Consob

Al riguardo il Garante si è espresso favorevolmente sulla modifica del regolamento per i trattamenti al riguardo effettuati dalla Commissione nazionale per le società e la borsa (Consob) resasi necessaria a seguito del mutato quadro normativo di riferimento, in particolare con l'istituzione dell'Arbitro per le controversie finanziarie (Acf) e a seguito dell'attuazione dell'art. 2, commi 5-*bis* e 5-*ter*, d.lgs. 8 ottobre 2007, n. 179, concernente i criteri di svolgimento delle procedure di risoluzione extra-giudiziale delle controversie presso l'Arbitro nonché di composizione del relativo organo decidente. In particolare, oltre ad una revisione del precedente regolamento, anche grazie all'interlocuzione con l'Ufficio sono state individuate le tipologie di dati sensibili e giudiziari trattati e le operazioni eseguibili nell'ambito dei nuovi trattamenti introdotti dalla novella normativa (parere 16 marzo 2017, n. 137, doc. web n. 6341897).

Garante per l'infanzia

Parere favorevole è stato reso anche sullo schema di regolamento per il trattamento dei dati sensibili e giudiziari effettuato dall'Autorità garante per l'infanzia e l'adolescenza volto ad individuare i tipi di dati sensibili e le operazioni eseguibili per lo svolgimento dei compiti di verifica del rispetto e della corretta attuazione della normativa a tutela dell'infanzia e dell'adolescenza. L'Autorità garante per l'infanzia può, infatti, a seguito di proprie istruttorie, venire a conoscenza della violazione o del rischio di violazione dei diritti delle persone di minore età, ivi comprese quelle riferibili ai mezzi di informazione, con conseguenti operazioni di trattamento, con eventuale segnalazione agli organismi cui sono attribuiti i poteri di controllo e sanzionatori. Nell'ambito dell'istruttoria particolare attenzione è stata posta sulla verifica dei presupposti normativi e delle garanzie da assicurare in relazione al trattamento di dati sensibili e giudiziari riferibili a soggetti minori e ai loro familiari, avuto riguardo anche alle competenze attribuite ai garanti regionali (parere 22 giugno 2017, n. 285, doc. web n. 6630330).

Inapp

Infine, è stato dato parere favorevole sulla modifica del regolamento concernente il trattamento dei dati sensibili e giudiziari effettuati presso l'Istituto nazionale per l'analisi delle politiche pubbliche (Inapp), dovuta, in particolare, alla necessità di inserire una nuova scheda che descrive dettagliatamente il trattamento di dati personali per scopi statistici. L'Inapp, infatti, fa parte del Sistema statistico nazionale per lo svolgimento dell'indagine sociale europea (ESS) - anno 2017, non inserita nel Programma statistico nazionale 2017-2019, ma solo nel relativo aggiornamento 2018-2019. Specifiche garanzie sono state individuate, d'intesa con l'Ufficio, con riferimento ai

tipi di dati sensibili trattati (dati idonei a rivelare l'origine etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché dati personali idonei a rivelare lo stato di salute) e le operazioni eseguibili. In particolare, si evidenzia che, per la conduzione dell'ESS, riferita a tutti gli individui di età superiore ai 14 anni residenti in Italia, è prevista la raccolta dei dati presso gli interessati su base volontaria, con l'adozione di idonee cautele in caso di soggetti rispondenti minorenni. In ogni caso, i dati sono resi anonimi al termine del trattamento statistico (parere 26 luglio 2017, n. 341, doc. web n. 6819856).

Dichiarazioni di appartenenza a gruppo linguistico

Chiarimenti sono stati forniti al Dipartimento per gli affari regionali della Presidenza del Consiglio dei ministri in merito al trattamento di dati personali effettuato in materia di previdenza e assicurazioni sociali ai sensi dell'art. 9, d.P.R. 6 gennaio 1978, n. 58 (Norme di attuazione dello Statuto speciale della Regione Trentino-Alto Adige in materia di previdenza e assicurazioni sociali). In particolare, il Dipartimento aveva chiesto se le organizzazioni sindacali, in base alla normativa di attuazione vigente, potessero raccogliere le dichiarazioni di appartenenza al gruppo linguistico dei propri iscritti e trasmetterle al Consiglio provinciale di Bolzano nell'ambito del procedimento di competenza relativo all'accertamento della maggiore rappresentatività della confederazione sindacale alla quale aderiscono le associazioni sindacali costituite tra lavoratori dipendenti appartenenti alle minoranze linguistiche tedesca e ladina. In relazione a tale problematica l'Autorità ha osservato che il d.P.R. 26 luglio 1976, n. 752 (Norme di attuazione dello Statuto speciale della Regione Trentino-Alto Adige in materia di proporzione negli uffici statali siti nella provincia di Bolzano e di conoscenza delle due lingue nel pubblico impiego), oggetto di importanti modifiche dovute anche al mutato quadro normativo europeo e nazionale in materia di protezione dei dati personali, delinea uno specifico apparato di garanzie per il trattamento dei dati relativi all'appartenenza/aggregazione ai tre gruppi linguistici (italiano, tedesco e ladino) in Provincia di Bolzano, prevedendone l'uso in casi tassativamente individuati e disciplinando rigorosamente le modalità di raccolta e di successivo trattamento delle dichiarazioni individuali nominative di appartenenza ai gruppi linguistici. In particolare, l'art. 20-*ter*, comma 3, dispone che il dichiarante produca la suddetta certificazione, in un plico chiuso, quando dichiara il possesso dei requisiti per accedere ai benefici previsti, il quale viene aperto solo nel momento dell'accertamento del possesso dei requisiti richiesti, facendo divieto di richiedere di produrre la certificazione in questione in casi e per finalità diverse da quelli tassativamente previsti per legge.

Più in generale, con riferimento al trattamento dei dati sensibili, quali quelli relativi all'appartenenza/aggregazione ai menzionati gruppi linguistici in Provincia di Bolzano, è stato evidenziato che il trattamento di tale tipologia di informazioni da parte di soggetti pubblici è consentito dal Codice solo se autorizzato da espressa disposizione di legge che specifichi la tipologia dei dati e le finalità perseguite. Nei casi in cui una disposizione di legge specifichi la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante. Inoltre, il trattamento dei dati sensibili deve avvenire nel rispetto dei principi di cui all'art. 22 del Codice, ai sensi del quale, in particolare, i soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato e possono trattare solo i dati sensibili e giudiziari indispen-

sabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi. Specifica attenzione è prestata inoltre alla verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

Con riferimento alla questione sottoposta all'Autorità, è stato pertanto rappresentato che, alla luce del quadro normativo vigente – che richiede, *in primis*, l'individuazione puntuale in via legislativa dei trattamenti di dati relativi all'appartenenza/ aggregazione ai tre gruppi linguistici –, non è stata rinvenuta, allo stato, una base giuridica idonea a legittimare l'ipotizzato trattamento di dati personali da parte delle organizzazioni sindacali e del Consiglio provinciale.

Per quanto concerne, invece, un possibile intervento del legislatore sull'istituto del sindacato maggiormente rappresentativo di cui all'art. 9, d.P.R. n. 58/1978 (come auspicato dal Trga di Bolzano), si è sottolineata la necessità che tale eventuale modifica avvenga nel rispetto dello specifico quadro di garanzie delineato dalla novellata disciplina di cui al citato d.P.R. n. 752/1976 e dalla normativa in materia di protezione dei dati personali.

Sul punto è stato evidenziato che anche il nuovo RGPD richiede l'adozione di idonee cautele per il trattamento di tale particolare categoria di dati personali, suscettibile di creare rischi significativi per i diritti e le libertà fondamentali. Più specificamente, il trattamento di tali dati deve essere necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve risultare proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. *g*), e considerando 51 e 52) (nota 14 dicembre 2017).

4.2. *La vigilanza sulle grandi banche dati pubbliche*

Le grandi banche dati pubbliche continuano a rientrare nell'attività di vigilanza dell'Autorità sia d'ufficio che a seguito di segnalazioni di interessati o in caso di comunicazione di *data breach*, talvolta con l'apertura di istruttorie che si concludono con l'introduzione, anche a seguito di prescrizioni del Garante, di misure volte ad irrobustire la sicurezza delle banche dati pubbliche, ovvero con la segnalazione, da parte del Garante, alle competenti Procure della Repubblica di accessi abusivi a sistema informatico ai sensi dell'art. 615-*ter*, c.p.

Data breach

Oltre a quanto illustrato in relazione ai controlli sull'Anagrafe tributaria in relazione all'attività fiscale (cfr. *infra* par. 4.5), è stato avviato uno specifico accertamento a seguito di un *data breach* riguardante i dati trattati mediante l'applicativo web "fatture e corrispettivi" dell'Agenzia delle entrate. È stato verificato, infatti, che alcune funzionalità di tale applicativo consentivano agli intermediari di accedere a informazioni relative anche a soggetti terzi (nota Presidente 3 ottobre 2017, doc. web n. 6918092).

Numerose segnalazioni e reclami hanno riguardato inoltre accessi ingiustificati ai sistemi informativi dell'Inps e all'Agenzia delle entrate da parte di dipendenti o di altri soggetti autorizzati, quali ad esempio operatori di patronati, volti ad acquisire illecitamente documentazione contributiva e fiscale.

Cad

Ancorché il Garante abbia espresso il parere del 29 novembre 2017, n. 436 (doc. web n. 7221785) sullo schema di decreto legislativo recante le disposizioni integrative e correttive al Cad (d.lgs. 13 dicembre 2017, n. 217) nei termini che si sono

anticipati (v. par. 2.1.2), nella versione definitiva di tale decreto è stata introdotta una disposizione – assente nello schema sottoposto al parere del Garante – con la quale è stata istituita una Piattaforma Digitale Nazionale Dati, affidata in via sperimentale al Commissario straordinario per l'attuazione dell'agenda digitale, presso la quale verrebbero potenzialmente accentrati e duplicati, per finalità del tutto generiche, tutti i dati detenuti dalle pp.aa. (art. 50-*ter* del Cad). In considerazione dell'impatto rilevantissimo che tale disposizione determina in relazione alla gestione dei dati personali trattati dalla p.a. e delle gravi preoccupazioni suscitate dalla stessa, in ragione dell'impatto senza precedenti sull'assetto delle garanzie assicurate fino a oggi nel trattamento dei dati personali nella p.a., anche a voler ritenere che la norma in parola sia in linea con la delega attribuita dal legislatore, il Garante (non essendosi potuto esprimere, per le ragioni enunciate, in sede di parere) ha segnalato con una nota al Presidente del Consiglio dei ministri le criticità rilevate, precisando che una modifica di tale importanza avrebbe richiesto certamente un ulteriore interpello dell'Autorità. In particolare, sono stati rappresentati i dubbi in ordine alla compatibilità con la normativa europea sulla protezione dei dati, poiché presso la suddetta piattaforma dovrebbero essere accentrati e duplicati tutti i dati detenuti dalle pp.aa. per finalità, come anticipato, del tutto generiche. Si realizzerebbe così un'inedita concentrazione presso un unico soggetto di informazioni personali, anche sensibili e sensibilissime, con evidenti rischi di usi distorti e accessi non autorizzati. Il ruolo affidato al Garante dalla suddetta disposizione non pare peraltro sufficiente a superare le criticità sopra evidenziate. È stato, infine, rappresentato che la pur necessaria valorizzazione del patrimonio informativo pubblico non deve avvenire a discapito della tutela dei diritti fondamentali e con possibili ricadute anche in termini di sicurezza nazionale (nota del Presidente 22 gennaio 2018, doc. web n. 8456134).

Spid

Sono proseguite le verifiche sullo Spid, con accertamenti ispettivi sia presso i gestori dell'identità digitale che presso alcuni fornitori di servizi, al fine di aggiornare e incrementare, anche in collaborazione con l'AgID nell'ambito della prevista attività di vigilanza, le cautele introdotte con la specifica normativa di attuazione.

A seguito di una segnalazione sono stati effettuati opportuni accertamenti al fine di incrementare i livelli delle misure di sicurezza del sito istituzionale del Ministero dei trasporti (www.ilportaledellautomobilista.it). Il Ministero ha fornito idonee rassicurazioni circa la potenziale vulnerabilità cui sarebbero esposti gli utenti utilizzatori di *app* di terze parti, provvedendo, in particolare, all'eliminazione in via prudenziale dei cifrari anonimi dalla configurazione del *server* web, se non tecnicamente necessari (nota 26 giugno 2017).

4.3. *La trasparenza amministrativa*

4.3.1. L'accesso civico

Tra le novità in materia di diritto di accesso e protezione dei dati personali si registrano svariati pareri resi ai responsabili della prevenzione della corruzione o a difensori civici ai sensi dell'art. 5, commi 7 e 8, d.lgs. n. 33/2013. Alla luce degli stessi è possibile effettuare un primo bilancio in ordine agli orientamenti espressi dal Garante su diverse fattispecie nelle quali si è invitata l'amministrazione a escludere l'accesso civico ai sensi dell'art. 5, comma 2-*bis*, lett. *a*), d.lgs. n. 33/2013, in presenza di un pregiudizio concreto alla protezione dei dati personali. Ciò anche considerando che i dati e i documenti che si ricevono a seguito di un'istanza di accesso civico – a differenza di quelli che si ricevono tramite l'accesso ai documenti amministrativi ai sensi della legge n. 241/1990 – divengono "pubblici e chiunque ha dirit-

to di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7", sebbene il loro ulteriore trattamento debba, in ogni caso, essere effettuato nel rispetto dei limiti derivanti dalla normativa in materia di protezione dei dati personali (art. 3, comma 1, d.lgs. n. 33/2013). È infatti anche alla luce di tale amplificato regime di pubblicità dell'accesso civico che va valutata l'esistenza di un possibile pregiudizio concreto alla protezione dei dati personali dei soggetti controinteressati, da coinvolgere nel procedimento relativo all'accesso civico ai sensi dell'art. 5, comma 5, d.lgs. n. 33/2013.

In tale quadro, sono comunque state tenute in considerazione le indicazioni contenute nelle linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5, comma 2, d.lgs. n. 33/2013 (determinazione Anac 28 dicembre 2016, n. 1309), adottate d'intesa con il Garante (provv. 15 dicembre 2016, n. 521, doc. web n. 5860807).

Dati sulla salute

Procedendo per ambiti nel dar conto dei casi più significativi, può essere evidenziato che, ai sensi dell'art. 5, comma 3, d.lgs. n. 33/2013, deve essere "escluso" l'accesso civico a dati idonei a rivelare lo stato di salute, in quanto per i predetti dati esiste uno specifico divieto di diffusione (art. 22, comma 8, del Codice e art. 7-*bis*, comma 6, d.lgs. n. 33/2013). In particolare, va escluso l'accesso civico a qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia, l'esistenza di una patologia oppure una condizione di invalidità, disabilità o handicap di una persona. Tale conclusione è stata raggiunta rispetto all'accesso all'elenco dei nominativi dei beneficiari di pensione privilegiata tabellare destinata al personale militare con infermità o lesioni dipendenti da fatti di servizio (prevista dall'art. 67, d.P.R. 29 dicembre 1973, n. 1092), in quanto la relativa ostensione avrebbe comportato la generale conoscenza di dati idonei a rivelare lo stato di salute dei soggetti interessati, per i quali è invece previsto un espresso divieto di diffusione da parte dei soggetti pubblici (parere 10 aprile 2017, n. 188, doc. web n. 6383249).

Dati relativi a situazioni di disagio economico-sociale

Ai sensi dell'art. 5, comma 3, d.lgs. n. 33/2013, è stato "escluso" l'accesso civico a dati identificativi di persone fisiche destinatarie dei provvedimenti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche, qualora da tali documenti sia possibile ricavare informazioni relative alla situazione di disagio economico-sociale degli interessati, atteso che anche per questi dati è previsto un espresso divieto di diffusione per finalità di trasparenza dall'art. 7-*bis*, comma 6, d.lgs. n. 33/2013 (parere 27 aprile 2017, n. 206, doc. web n. 6388689).

Minorenni

A fronte di una richiesta di parere avente ad oggetto un'istanza di accesso civico volta a ottenere l'estrazione in formato elettronico della documentazione relativa ai registri attestanti le presenze e le assenze di tutti gli alunni (minorenni) di un istituto scolastico – aggregante scuola dell'infanzia, primaria e secondaria di primo grado (informazione già di per sé di natura riservata considerando la vulnerabilità dei soggetti interessati) nell'arco temporale corrispondente a due anni scolastici – nonché ulteriori dati e informazioni di contesto parimenti delicati (come quelli relativi a tutti i giorni di presenza o assenza scolastica di ogni singolo alunno, riferiti agli ultimi 3 anni), è stato ritenuto corretto il rifiuto dell'istituto scolastico. Ciò considerata la natura, la specie e la quantità dei dati personali richiesti riferiti a soggetti minorenni e il richiamato regime di pubblicità dei dati e documenti oggetti di accesso civico (art. 3, comma 1, d.lgs. n. 33/2013) con conseguente pregiudizio concreto al diritto alla protezione dei dati personali dei minori (parere 16 novembre 2017, n. 476, doc. web n. 7273244).

Dati dei dipendenti

In più di un caso il Garante ha evidenziato che l'accesso civico in ambito lavorativo a dati e informazioni riguardanti i dipendenti e la relativa attività lavorativa – quali provvedimenti e sanzioni disciplinari, presenze al lavoro, permessi, ferie, orari

di ingresso e di uscita risultanti dal *badge*, atti dei concorsi e provvedimenti di assunzione, segnalazioni o provvedimenti per conflitto di interesse – va rifiutato in quanto l'ostensione dei predetti documenti e informazioni è suscettibile di determinare, a seconda delle ipotesi e del contesto in cui possono essere utilizzati da terzi, un pregiudizio concreto alla tutela della protezione dei dati personali (pareri 9 febbraio 2017, n. 50, doc. web n. 6057812; 31 maggio 2017, n. 254, doc. web n. 6495493; 13 settembre 2017, n. 369, doc. web n. 7155944).

Il Garante ha ribadito tale orientamento anche in relazione alla richiesta di conoscere la presenza o meno in servizio, in date determinate, di un ex dipendente di una Fondazione Ircss, considerate le ragionevoli aspettative di confidenzialità del lavoratore e indipendentemente dalla circostanza della intervenuta cessazione del rapporto di servizio con la predetta Fondazione (parere 10 aprile 2017, n. 190, doc. web n. 6383028).

In un altro caso poi, in ordine alla richiesta di accesso civico all'intera documentazione afferente alla valutazione delle *performance* dirigenziali relativa ad uno specifico biennio (comprese le valutazioni di competenza dell'Oiv, del Segretario generale, le relazioni formulate e i dati comunicati dai dipendenti a supporto dell'attività dagli stessi realizzate), è stato valutato che la relativa ostensione avrebbe potuto arrecare ai soggetti interessati un pregiudizio concreto alla tutela della protezione dei dati personali. In ogni caso, è stato evidenziato che restano fermi i puntuali obblighi di pubblicazione *online* previsti per espressa finalità di trasparenza dagli artt. 14, comma 1-*ter* e 20, d.lgs. n. 33/2013, relativi all'attività delle pp.aa. e alla valutazione della *performance*, nonché alla distribuzione dei premi al personale dirigenziale, che lo stesso legislatore, nel rispetto del principio di proporzionalità di cui all'art. 11 del Codice, ha ritenuto idonei a soddisfare l'esigenza conoscitiva della collettività, strumentale al perseguimento delle finalità dell'accesso civico di cui all'art. 5, comma 2, d.lgs. n. 33/2013 (parere 29 dicembre 2017, n. 574, doc. web n. 7658152).

In alcuni casi, invece, il Garante ha richiamato l'attenzione delle pp.aa. sulla possibilità di far conoscere tramite l'accesso civico alcune informazioni grazie ad un accesso civico parziale.

In particolare, tale ragionamento è stato fatto in relazione alla richiesta di ostensione di un ordine di servizio riguardante le competenze attribuite al dirigente vicario presso un provveditorato regionale del Dipartimento dell'amministrazione penitenziaria. In tale fattispecie il Garante ha invitato l'amministrazione a valutare la possibilità di consentire l'accesso civico alla parte del predetto ordine di servizio relativa all'affidamento di competenze e funzioni che fossero risultate omogenee rispetto a quelle per le quali era previsto un onere di trasparenza ai sensi degli artt. 13 e 14, comma 1-*bis*, d.lgs. n. 33/2013 (parere 4 maggio 2017, n. 214, doc. web n. 6388380).

Analogamente, in relazione alla richiesta di accesso civico avanzata nei confronti di una società di servizio pubblico locale avente a oggetto gli obiettivi assegnati ai quadri aziendali e la natura ed entità delle indennità erogate, si è richiamata la possibilità di accogliere parzialmente l'accesso, procedendo però all'oscuramento di tutti i dati personali dei soggetti interessati (ivi comprese le informazioni idonee a identificarli, anche indirettamente), oppure fornendo i dati in forma aggregata (parere 10 aprile 2017, n. 189, doc. web n. 6383094).

***Curricula* e manifestazioni di interesse**

È stato evidenziato che l'eventuale accoglimento di una richiesta di accesso civico alle manifestazioni di interesse a una particolare posizione lavorativa presso un ministero, effettuata inviando il *curriculum vitae* (redatto, in ogni suo campo, secondo il modello europeo) poteva arrecare un pregiudizio concreto alla tutela della protezione dei dati personali, anche considerando che nell'avviso per la raccolta delle predette manifestazioni di interesse era espressamente previsto che non sarebbe stato reso pubblico l'elenco di coloro che avrebbero presentato il proprio *curriculum*, generando in

tal modo ragionevoli aspettative di riservatezza in capo agli interessati riguardo al trattamento dei dati personali loro riferiti. È stato peraltro evidenziato che la presenza nel *curriculum vitae* di dati e informazioni dettagliati degli interessati rende particolarmente difficile, se non impossibile, l'anonimizzazione del documento, con la conseguenza di impedire anche un eventuale accesso civico parziale ai sensi dell'art. 5-*bis*, comma 4, d.lgs. n. 33/2013 (parere 30 marzo 2017, n. 162, doc. web n. 6393422).

Dati relativi a concorsi pubblici

In tema di concorsi pubblici il Garante è intervenuto in più occasioni, evidenziando che in alcuni casi per alcuni specifici documenti (quali i verbali redatti dalla commissione relativi allo svolgimento delle prove scritte di un concorso) è possibile accordare un accesso parziale, mediante oscuramento dei dati personali e di tutte le altre informazioni idonee a identificare, anche indirettamente, i soggetti interessati presenti nei citati documenti (es.: nominativi dei candidati che hanno sorteggiato le tracce, che sono stati esclusi, che si sono ritirati, ecc.).

Al contrario, va in ogni caso negato l'accesso civico ai documenti relativi alle prove scritte e orali svolte dai candidati con la relativa votazione, nonché alla valutazione dei titoli, in quanto l'ostensione potrebbe determinare, a seconda delle ipotesi e del contesto in cui le informazioni possono essere utilizzate da terzi, un pregiudizio alla protezione dei dati personali (parere 7 settembre 2017, n. 366, doc. web n. 7155171).

Analogamente è stato rappresentato che la richiesta di accesso generalizzato agli elaborati di un concorso e alle rispettive valutazioni (peraltro da parte di soggetto non partecipante al concorso) andava respinta a mente del fatto che l'elaborato scritto è, in linea di massima, indicativo di molteplici aspetti di carattere personale circa le caratteristiche individuali, ad esempio relative alla preparazione professionale, alla cultura, alle capacità espressive, o al carattere del candidato, aspetti suscettibili di valutazione nella selezione dei partecipanti. Inoltre, in alcuni casi, e a seconda della traccia sottoposta, il contenuto degli elaborati può essere potenzialmente capace di rivelare anche informazioni e convinzioni che possono rientrare nella categoria dei dati sensibili di cui all'art. 4, comma 1, lett. *d*), del Codice (si pensi in particolare alle tracce su temi storici o di cultura generale che potrebbero rivelare "opinioni politiche", "convinzioni filosofiche o di altro genere").

È stata altresì evidenziata l'impossibilità di accordare anche solo un accesso civico parziale, fornendo la copia degli elaborati priva dell'associazione ai dati personali identificativi dei candidati. Ciò in quanto, anche se la correzione dei compiti delle procedure concorsuali avviene in modo anonimo, la particolare circostanza che l'elaborato scritto è redatto di proprio pugno dal candidato, non elimina completamente la possibilità, tutt'altro che remota, che – una volta reso pubblico l'elaborato tramite l'accesso civico – il soggetto interessato possa essere re-indentificato a posteriori tramite la conoscenza o la comparazione della relativa grafia (cfr. la definizione di "dato personale" contenuta nell'art. 4, par. 1, n. 1, RGPD). Il Garante ha, infine, richiamato l'attenzione dell'amministrazione sulla necessità di valutare – considerando il richiamato regime di pubblicità dei documenti forniti in sede di accesso civico e la circostanza che l'elaborato è il risultato di un'opera intellettuale del candidato – l'esistenza di ulteriori interessi privati per potrebbero portare a escludere l'accesso civico, previsti dall'art. 5-*bis*, comma 2, lett. *c*), legati, ad esempio, all'esistenza di interessi legati alla proprietà intellettuale o al diritto d'autore (pareri 26 ottobre 2017, n. 433, doc. web n. 7156158 e 24 maggio 2017, n. 246, doc. web n. 6495600).

Procedimenti di accertamento e sanzionatori

È stato ritenuto corretto il rifiuto dell'accesso civico opposto da un Dipartimento del Garante a una richiesta avente a oggetto atti detenuti dall'amministrazione relativi alle comunicazioni ricevute da una società e ai relativi procedimenti di accertamento e di irrogazione della sanzione amministrativa. Ciò sulla

base dell'esigenza di evitare un pregiudizio concreto alla protezione dei dati personali, in conformità con la disciplina legislativa in materia (art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013) e alla luce dell'esclusione prevista dal Regolamento n. 1/2006 del Garante (che, ai sensi dell'art. 5-*bis*, comma 3, d.lgs. n. 33/2013, porta a escludere anche l'accesso civico). Nei citati atti comparivano, infatti, dati identificativi di dipendenti e collaboratori della società nonché, con riferimento al procedimento sanzionatorio, dati personali riferiti a soggetti segnalanti o coinvolti nelle verifiche. Inoltre, la presenza di informazioni aziendali, tecnico-industriali, commerciali, organizzative e finanziarie, attinenti al *know-how* aziendale non rendeva possibile accordare neppure un accesso parziale (parere 26 ottobre 2017, n. 434, doc. web n. 7156279).

Titoli abilitativi edilizi: Scia e Cila

È stato ritenuto corretto il diniego dell'accesso civico opposto da un comune alle segnalazioni certificate di inizio attività (Scia) e alle comunicazioni inizio lavori asseverata (Cila). Ciò in quanto l'ostensione dei predetti documenti o informazioni, considerata la quantità e qualità dei dati personali coinvolti, unitamente al particolare regime di pubblicità dei medesimi dati, è stato ritenuto suscettibile di determinare, a seconda delle ipotesi e del contesto in cui possono essere utilizzati da terzi, un pregiudizio concreto alla tutela della protezione dei dati personali.

Il Garante ha evidenziato che il medesimo pregiudizio poteva realizzarsi anche nel caso di un eventuale e più limitato accesso civico parziale, avente a oggetto i soli dati del tecnico progettista (senza quelli relativi al committente), corredati però dalla descrizione dell'intervento e della località dove avveniva il lavoro con via e numero civico. Anche in questo caso è stato ritenuto corretto quanto evidenziato dal comune destinatario della richiesta di accesso civico, laddove è stato sostenuto che dai dati in questione era possibile risalire all'esistenza del rapporto professionale tra committente e progettista e che anche se si fossero oscurati i dati del committente, l'indicazione dell'immobile oggetto dell'intervento avrebbe consentito di risalire all'identità del relativo proprietario tramite una visura catastale.

Il Garante ha inoltre evidenziato che la conoscenza indiscriminata dell'ampio *set* di informazioni e dati personali contenuti nella documentazione oggetto dell'accesso civico (Cila e Scia) appariva non necessaria o risultava comunque sproporzionata rispetto allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico. Per tali scopi, nell'ambito di un controllo sul complessivo esercizio delle funzioni amministrative del comune in materia edilizia e di un eventuale dibattito pubblico in materia, potevano eventualmente essere utili dati statistici riguardanti il numero e la tipologia degli atti o la tipologia degli interventi, mentre lo stesso non poteva dirsi, ad esempio, per le generalità dei singoli committenti e progettisti (pareri 10 agosto 2017, n. 360, doc. web n. 6969290; 18 agosto 2017; n. 361, doc. web n. 6969198 e 1° settembre 2017, n. 364, doc. web n. 6979969).

Elenchi di contribuenti Imu

È stato esaminato il caso della richiesta di accesso civico a due elenchi: a) quello dei contribuenti di un comune che avevano versato l'imposta municipale unica (Imu) sulla prima casa negli ultimi tre anni (a partire dall'anno 2014); b) quello degli immobili a uso residenziale prima casa siti nel medesimo comune per i quali nel predetto periodo di tempo era stata corrisposta la citata imposta.

L'ostensione dei dati richiesti con l'accesso civico avrebbe fornito una grande quantità di informazioni personali relative ai proprietari – che dalle stime del comune riguardavano più di 2.000 immobili – di natura e specie diversa. Infatti, oltre ai dati identificativi dei soggetti interessati, era possibile desumere dati come la residenza in un certo comune, l'aver fissato in quell'immobile la propria abitazione principale, la qualità di "proprietario" di un immobile di una certa tipologia con l'i-

dentificazione dell'immobile stesso, l'aver versato o meno uno specifico tributo. Inoltre, poiché i soggetti tenuti a pagare l'Imu nel comune sono quelli che hanno l'abitazione principale negli immobili situati nel predetto comune appartenenti alle categorie catastali A/1, A/8 e A/9, l'informazione sui contribuenti richiesta era idonea a rivelare anche ulteriori elementi, come il tenore di vita o la situazione patrimoniale dei soggetti interessati.

Per tali motivi, è stato ritenuto che l'amministrazione abbia correttamente respinto l'istanza di accesso civico, in quanto l'ostensione dei dati e delle informazioni richiesti era suscettibile di determinare, a seconda delle ipotesi e del contesto in cui possono essere utilizzati da terzi, un pregiudizio concreto alla tutela della protezione dei dati personali dei soggetti interessati.

È stata inoltre ritenuta non praticabile la possibilità di fornire un accesso civico parziale, limitato al solo elenco dei più di 2.000 immobili a uso residenziale prima casa siti nel comune per i quali nel predetto periodo di tempo è stata corrisposta l'Imu, priva dell'elenco dei soggetti che hanno corrisposto il tributo. Ciò in quanto l'ostensione di tali informazioni non avrebbe del tutto escluso l'identificazione indiretta dei proprietari mediante il collegamento con altre banche dati (es., banca dati catastale, pagine bianche, etc.) (parere 30 novembre 2017, n. 506, doc. web n. 7316508).

Conferimento di onorificenze

Con riguardo all'istanza di accesso civico avente a oggetto la documentazione della Presidenza del Consiglio dei ministri, detenuta dall'ufficio del cerimoniale di Stato e per le onorificenze, relativa all'istruttoria inerente alla proposta al Presidente della Repubblica di un'attribuzione dell'onorificenza di "Cavaliere", è stato ritenuto che, anche considerando la diversa specie e natura dati personali ivi contenuti, l'ostensione della documentazione richiesta, unita alla generale conoscenza e al particolare regime di pubblicità dei dati oggetto di accesso civico, avrebbe potuto arrecare al soggetto interessato, a seconda delle ipotesi e del contesto in cui le informazioni fornite avrebbero potuto essere utilizzate da terzi, un pregiudizio concreto alla tutela della protezione dei dati personali. Nel caso di specie, inoltre, la Presidenza del Consiglio dei ministri aveva evidenziato che il conferimento dell'onorificenza era un atto discrezionale, rientrante nelle prerogative del Presidente della Repubblica e, come tale, non sindacabile. Peraltro, il d.P.C.M. 27 giugno 2011, n. 143 prevede l'esclusione dell'accesso documentale di tutta la documentazione riguardante il conferimento di onorificenze, con la conseguente applicazione di una delle ipotesi di esclusione dell'accesso civico ai sensi dell'art. 5-*bis*, comma 3, d.lgs. n. 33/2013 (parere 29 dicembre 2017, n. 566, doc. web n. 7658205).

Verbali del Comitato unico di garanzia

In relazione a un'istanza di accesso civico a diversi verbali detenuti da un comune, redatti dal Comitato unico di garanzia delle pari opportunità, la valorizzazione del benessere di chi lavora e contro le discriminazioni istituito ai sensi dell'art. 57, d.lgs. 30 marzo 2001, n. 165, considerando che i predetti verbali risultavano contenere dati e informazioni personali di dipendenti (anche puntuali e di natura delicata, legati all'attività e all'ambiente lavorativo nonché alla ricezione di segnalazioni e all'adozione di provvedimenti disciplinari), è stato ritenuto che l'amministrazione abbia correttamente rifiutato l'accesso civico; quest'ultimo avrebbe infatti potuto esporre i controinteressati a ipotetiche ritorsioni e/o vessazioni, con ulteriore pregiudizio al clima lavorativo, in violazione del diritto alla protezione dei dati personali.

Le predette considerazioni hanno altresì impedito di accordare un accesso civico parziale ai documenti in questione, tramite oscuramento dei nominativi delle persone interessate, in quanto il predetto accorgimento tecnico non avrebbe eliminato completamente la possibilità di re-identificazione dei soggetti menzionati

attraverso il complesso delle vicende descritte e le ulteriori informazioni contenute nei documenti di cui è stata negata l'ostensione, considerate le ridotte dimensioni del comune in questione (parere 14 dicembre 2017, n. 528, doc. web n. 7450772).

Segnalazioni di illeciti al Garante

È stato esaminato l'accesso civico avente a oggetto segnalazioni, contenenti dati e informazioni personali, inviate da persone fisiche al Garante. In tal caso, è stato ritenuto corretto il rifiuto opposto all'accesso civico, sulla base dell'esigenza di evitare un pregiudizio concreto alla protezione dei dati personali, in conformità con la disciplina legislativa in materia (art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013) nonché alla luce dell'esclusione prevista dal Regolamento n. 1/2006 del Garante, ai sensi dell'art. 5-*bis*, comma 3, d.lgs. n. 33/2013 (parere 9 novembre 2017, n. 459, doc. web n. 7156608).

Visite di controllo domiciliare

Il Garante ha ritenuto che, fermo restando la possibilità di esercitare il diritto di accesso ai documenti amministrativi ai sensi della legge n. 241/1990, la richiesta di accesso civico, proposta da un ex dipendente, volta a conoscere il nominativo e il numero di matricola del medico Inps che non era riuscito a effettuare la visita medica di controllo domiciliare perché il lavoratore risultava assente, andava respinto, in ragione del ruolo svolto dai medici fiscali e del regime di pubblicità a cui sono sottoposti i dati e i documenti oggetto di accesso civico; la conoscibilità dei dati richiesti avrebbe potuto comportare eventuali conseguenze sulla sicurezza ed incolumità fisica degli interessati e, comunque, avere impatto negativo sul piano morale, relazionale e sociale (in termini, ad es., di ritorsioni, minacce, intimidazioni) (parere 2 novembre 2017, n. 458, doc. web n. 7158911).

Atti notarili, visure catastali e ipotecarie

Il Garante ha ritenuto che il Consiglio notarile abbia correttamente respinto l'istanza di accesso civico avente a oggetto copia di tutti gli atti notarili, delle visure catastali o delle visure ipotecarie trasmessi dai notai al Consiglio notarile nell'esercizio della propria attività di vigilanza. Ciò in quanto il relativo accoglimento avrebbe potuto arrecare un pregiudizio concreto alla protezione dei dati personali delle persone ivi indicate; inoltre, la richiesta di accesso civico alla copia di atti notarili, visure catastali e ipotecarie laddove presentata al soggetto/ufficio addetto alla conservazione del documento o al rilascio delle relative copie – quali archivio notarile, catasto, Agenzie delle entrate, etc. – ricade nelle ipotesi di esclusione dell'accesso civico di cui all'art. 5-*bis*, comma 3, d.lgs. n. 33/2013, in quanto il relativo accesso risulta disciplinato da specifiche discipline di settore che ne regolano le forme e modalità di rilascio, prevedendo, in alcuni casi, anche il pagamento di diritti o tributi (parere 21 settembre 2017, n. 377, doc. web n. 6919162).

Autocertificazione resa da un commissario straordinario

Il Garante ha evidenziato che è necessario valutare la possibilità di concedere un accesso civico parziale – mediante oscuramento dei dati personali eccedenti (quali data e luogo di nascita, domicilio, telefono, fax, *e-mail* e firma autografa) – alla richiesta di ottenere copia della dichiarazione resa ai sensi del d.P.R. n. 445/2000 da un commissario straordinario di una società ammessa alla procedura di amministrazione straordinaria contenente le dichiarazioni relative al possesso dei requisiti di professionalità e di onorabilità, all'inesistenza di cause impeditive e di incompatibilità o di situazioni di conflitto di interesse, e all'inesistenza di condanne per i reati previsti, dell'applicazione di misure di prevenzione e di procedimenti penali o azioni giudiziarie civili e penali pendenti. Ciò considerando il ruolo esercitato dal commissario straordinario e la rilevanza pubblica che assume la procedura di amministrazione straordinaria nonché la circostanza che nel caso di specie la dichiarazione presentata dal commissario straordinario non contenesse alcun riferimento a dati sensibili o giudiziari (parere 18 agosto 2017, n. 363, doc. web n. 6947348).

Revoca dell'incarico di commissario straordinario

L'accesso civico avente ad oggetto atti dell'istruttoria relativa alla revoca, con decreto ministeriale, dell'incarico di due commissari straordinari di società

ammesse a procedura di amministrazione straordinaria, fra cui note, verbali, osservazioni, controdeduzioni, *e-mail*, istanze e altri documenti contenenti dati e informazioni personali di varia natura, è suscettibile di determinare, a seconda delle ipotesi e del contesto in cui possono essere utilizzati da terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali di cui all'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013, anche in ragione del fatto che sulla questione risultava pendente un procedimento penale (parere 18 agosto 2017, n. 362, doc. web n. 6946925).

Costi e dati contabili

In relazione alla richiesta di accesso civico relativo ai costi sostenuti da un ente pubblico economico per gli acquisti e alla tipologia del materiale acquistato (riportati nei partitari contabili), si è ritenuto che l'amministrazione debba valutare la possibilità di accordare un accesso civico parziale, anonimizzando la documentazione richiesta, con l'esclusione dall'accesso dei dati personali e delle altre informazioni idonee a identificare, anche indirettamente, i soggetti interessati (parere 20 luglio 2017, n. 320, doc. web n. 6843143).

Comunicazione di avvio del procedimento amministrativo

È stato evidenziato che la generale conoscenza tramite l'istituto dell'accesso civico dei dati personali contenuti nella comunicazione di avvio del procedimento attivato dalla p.a. a seguito di una denuncia per opere edilizie realizzate in difformità alla normativa vigente (procedura peraltro archiviata dal comune destinatario dell'accesso), possa integrare, a seconda delle ipotesi e del contesto in cui le informazioni fornite possono essere utilizzate da terzi, un pregiudizio concreto alla tutela della protezione dei dati personali del soggetto controinteressato (parere 28 giugno 2017, n. 295, doc. web n. 6693221).

Dati di persone giuridiche

Il Garante ha evidenziato che – ai sensi dell'art. 4, comma 1, lett. *b*), del Codice – sono sottratte dall'ambito di applicazione della disciplina in materia di protezione dei dati personali le persone giuridiche, gli enti e le associazioni, che non possono beneficiare della tutela di cui al citato art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013. Pertanto, è stato rappresentato all'ente destinatario dell'istanza di valutare se la documentazione richiesta (verbali delle sedute del consiglio di amministrazione di una società ed elenco di esercizi commerciali che hanno ricevuto sanzioni amministrative) contenesse dati riferiti a persone fisiche, la cui ostensione avrebbe potuto determinare in concreto un pregiudizio allo loro riservatezza. La ritenuta sussistenza di tale pregiudizio doveva comportare il rigetto dell'istanza, salva la possibilità di accoglimento previo oscuramento dei dati personali eventualmente presenti e delle altre informazioni idonee ad identificare, anche indirettamente, i soggetti interessati (pareri 9 febbraio 2017, n. 49, doc. web n. 6057874; 16 febbraio 2017, n. 58, doc. web n. 6057387).

4.3.2. La pubblicazione di dati personali online

In materia di diffusione di dati personali *online* per finalità di trasparenza o di pubblicità dell'azione amministrativa, l'Autorità è stata chiamata a pronunciarsi su numerose questioni, di cui si riportano di seguito solo i casi più rilevanti definiti con provvedimento del Garante. In particolare, si è nuovamente presentato il problema della diffusione *online* di dati idonei a rivelare lo stato salute da parte di soggetti pubblici. Il Garante ha in proposito censurato il comportamento di un comune che aveva pubblicato, nella sezione "Amministrazione trasparente" del sito web istituzionale, diverse ordinanze del sindaco aventi ad oggetto la sottoposizione a trattamento sanitario obbligatorio, con indicazione in chiaro di una molteplicità di informazioni di dettaglio, quali il destinatario della richiesta, data e luogo di nascita, indirizzo di residenza, talora struttura ospedaliera presso la quale è stato ordinato il ricovero nonché circostanze ulteriori (provv. 2 marzo 2017, n. 88, doc. web n. 6285030).

Al riguardo, è stato ricordato che nel trattamento dei dati effettuato dai soggetti pubblici, i "dati idonei a rivelare lo stato di salute non possono essere diffusi" (art. 22, comma 8, del Codice), con la conseguenza che risulta vietata la diffusione di qualsiasi dato da cui possa desumersi 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 (art. 22, comma 8, nonché art. 65, comma 5, e art. 68, comma 3, del Codice; v. pure provv. 15 maggio 2014, n. 243, doc. web n. 3134436, "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").

Identiche considerazioni sono state svolte con riferimento alla pubblicazione effettuata da un comune sull'albo pretorio *online*, caso nel quale l'amministrazione aveva pubblicato il provvedimento di rilascio di un permesso per la chiusura con vetrate atermiche della tettoia posta sul lastrico solare di un immobile – di cui erano indicati indirizzo e dati catastali – al fine di destinarla a spazio dedicato alla riabilitazione di portatore di handicap, in applicazione di quanto previsto dalla legge della Regione Puglia 10 dicembre 2012, n. 39 (Abbattimento delle barriere architettoniche mediante realizzazione di ambienti per persone con disabilità grave negli edifici di edilizia residenziale in proprietà). Nel caso di specie, il destinatario del permesso di costruire citato nel provvedimento aveva rappresentato che lo stesso era finalizzato all'esecuzione di lavori a beneficio della figlia minore affetta da un grave handicap.

È stato pertanto ricordato che, in relazione alla possibilità di identificare anche indirettamente il soggetto interessato, in particolari ambiti (ad es., per campioni di popolazioni di ridotte dimensioni), la pubblicazione *online* anche solo di alcuni dati – quali la residenza o la complessiva vicenda oggetto di pubblicazione – è sufficiente a individuare univocamente la persona cui le stesse si riferiscono e, quindi, a rendere tale soggetto identificabile mediante il collegamento con altre informazioni che possono anche essere nella disponibilità di terzi o ricavabili da altre fonti. Per rendere effettivamente anonimi i dati pubblicati *online* occorre quindi oscurare del tutto il nominativo e le altre informazioni riferite all'interessato che ne possono consentire l'identificazione anche a posteriori (parte prima, par. 3, delle 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, cit.).

È stato quindi ritenuto che la pubblicazione sul sito web istituzionale del comune del provvedimento contente il permesso per effettuare lavori a beneficio della minorenne affetta da un grave handicap ha causato una diffusione di dati idonei a rivelare lo stato di salute, in violazione dell'art. 22, comma 8, del Codice. Ciò in quanto il predetto provvedimento riportava in chiaro dati e informazioni che consentivano di identificare indirettamente il soggetto portatore di handicap, quali: il nominativo del soggetto richiedente il permesso di costruire a favore del soggetto affetto da handicap, l'indirizzo di residenza e i dati catastali, gli estremi della normativa regionale di riferimento (provv. 5 luglio 2017, n. 303, doc. web n. 6946686).

4.4. *L'istruzione scolastica*

Nel settore scolastico il Garante si è confrontato con il Miur e con le università e le Istituzioni scolastiche nel corso di numerosi incontri e contatti volti a fornire

chiarimenti e indicazioni in merito alla corretta applicazione della disciplina in materia di protezione dei dati.

Tra gli atti più significativi si segnala il provvedimento 5 luglio 2017, n. 301 (doc. web n. 6843964) con il quale è stato espresso parere favorevole sullo schema di decreto del Miur volto a riordinare, in un unico provvedimento, l'insieme delle disposizioni secondarie concernenti l'Anagrafe Nazionale degli Studenti (Ans), intervenute successivamente all'emanazione del d.m. 5 agosto 2010, n. 74. L'Ans, istituita presso il Miur in base all'art. 3, d.lgs. 15 aprile 2005, n. 76, contiene i dati sui percorsi scolastici, formativi e di apprendistato dei singoli studenti, nonché quelli relativi alla loro valutazione a partire dal primo anno della scuola primaria.

Il d.m. n. 74/2010 è stato negli anni oggetto di numerosi interventi (cfr. d.m. 25 gennaio 2016, n. 24; d.m. 26 luglio 2016, n. 595; d.m. 9 novembre 2016, n. 862), i quali hanno progressivamente ampliato le informazioni contenute nell'Ans, prevedendo l'inserimento dei dati degli alunni frequentanti le scuole dell'infanzia appartenenti al sistema nazionale di istruzione, i dati relativi agli alunni disabili (in una partizione separata) e, infine, la definizione del tempo di conservazione delle informazioni concernenti gli esiti finali della scuola secondaria di secondo grado.

Facendo seguito alle osservazioni rese dall'Autorità, il Ministero ha riformulato lo schema di decreto, precisando che: l'Ans, la cui titolarità del trattamento viene attribuita al Miur, si configura non come soggetto giuridico, ma quale strumento di supporto per l'espletamento dei compiti conferiti dalle norme ai soggetti istituzionalmente competenti in materia; nelle more della definizione di un mezzo di identificazione d'uso generale nell'ambito delle pp.aa., lo studente viene identificato nell'Ans attraverso un codice meccanografico assegnato dal sistema al momento del primo inserimento dello stesso in anagrafe; al fine di monitorare l'evasione dall'obbligo di istruzione e la regolare frequenza scolastica, il Miur e le Istituzioni scolastiche possono consultare i dati contenuti nella Ans solo in forma aggregata.

Infine, sono state meglio specificate le misure tecniche e organizzative adottate a protezione dei dati degli alunni contenuti nell'Ans, rendendo maggiormente dettagliata la descrizione di taluni profili utente e aggiornando lo schema logico del servizio di autenticazione per comprendere tutti i soggetti coinvolti.

Nel corso dell'anno sono state altresì rilevate talune criticità nella modalità di redazione, da parte degli istituti scolastici, del cd. documento del 15 maggio, di cui all'art. 5, comma 2, d.P.R. 23 luglio 1998, n. 323, che hanno dato luogo ad ingiustificate diffusioni di dati personali riferiti a studenti, anche in internet. Il menzionato documento viene elaborato dai consigli di classe, entro il 15 maggio di ogni anno scolastico, al fine di consentire alla commissione esaminatrice di predisporre il testo della terza prova degli esami di Stato e descrive il percorso formativo e didattico e gli obiettivi raggiunti dalla classe. Tale documento, in base alla disciplina di settore, deve essere affisso all'albo dell'istituto e consegnato in copia a ciascun candidato. A seguito dell'entrata in vigore della legge n. 69/2009 – secondo cui gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione da parte delle amministrazioni nei siti internet istituzionali – taluni istituti scolastici hanno erroneamente ritenuto di dover pubblicare i predetti documenti, contenenti numerose informazioni riferite agli studenti, sul sito internet istituzionale con conseguente indicizzazione in rete del documento. Tale prassi non risulta tuttavia conforme alla disciplina in materia di protezione dei dati personali e, al fine di evitare ulteriori indebite diffusione di dati personali degli studenti, sono state fornite al Miur indicazioni operative al fine di conformare le modalità di redazione del documento del 15 maggio ai principi in materia di protezione dei dati personali (nota 21 marzo 2017).

Sempre con riferimento alla pubblicazione *online* di dati degli studenti, è inoltre pervenuta una segnalazione con la quale è stato rappresentato che, nel pubblicare gli esiti degli esami di Stato sull'albo e sul sito internet istituzionale, un istituto scolastico, avrebbe indicato anche l'indirizzo d'abitazione, la *e-mail* e/o il numero di telefono degli studenti interessati. Tale pubblicazione sarebbe stata effettuata nell'ambito dell'attività di intermediazione effettuata dagli istituti di scuola secondaria di secondo grado in attuazione dell'art. 6, d.lgs. 10 settembre 2003, n. 276.

A seguito dell'istruttoria preliminare, il Garante ha rilevato alcune specifiche criticità nelle modalità attuative della richiamata attività di intermediazione, avuto riguardo, in particolare, alla possibilità di pubblicare i *curricula* degli studenti prescindendo dal consenso degli stessi. È stato evidenziato che la pubblicazione dei *curricula* degli studenti ad opera dei soggetti legittimati, avvenendo nell'ambito di un'attività di intermediazione – intesa come attività volta a favorire l'incontro tra la domanda di lavoro, orientamento professionale o attività formative di uno specifico committente e l'offerta disponibile sul mercato – non possa essere disposta d'ufficio dal titolare del trattamento ma necessita di una esplicita richiesta dello studente. È stato altresì chiarito che, in maniera similare, anche la disposizione di cui all'art. 96, comma 1, del Codice, individua nell'esplicita richiesta da parte degli interessati, o degli esercenti la potestà genitoriale, il presupposto giuridico idoneo a legittimare la comunicazione o diffusione di dati personali degli studenti per finalità di orientamento, formazione e inserimento professionale.

Con riferimento inoltre ai tempi di diffusione del *curriculum* dello studente in relazione all'attività di intermediazione, il Garante, richiamando il principio di proporzionalità, ha chiarito che la pubblicazione di dati personali degli studenti possa essere effettuata soltanto per il tempo necessario e appropriato rispetto all'obiettivo perseguito. Tale lasso temporale è espressamente individuato dalla legge in almeno 12 mesi. Gli intermediari, pertanto, possono diffondere i richiamati dati personali riferiti agli alunni per un periodo di tempo superiore solo su esplicita richiesta del soggetto interessato (nota 16 marzo 2017).

4.5. *L'attività fiscale e tributaria*

Audit

È proseguita l'attività di vigilanza del Garante sull'osservanza delle norme in materia di protezione dei dati personali nelle procedure di registrazione degli accessi e di *audit* predisposte dalla Agenzia delle entrate per gli accessi ai dati personali contenuti nell'Anagrafe tributaria al fine di definire un quadro rafforzato di misure volte a prevenire accessi non autorizzati e trattamenti illeciti dei dati personali, nonché sui principi di qualità dei dati (pertinenza e non eccedenza, esattezza e aggiornamento). In particolare, l'Autorità ha preso atto del progetto organico per l'incremento dei livelli di sicurezza dell'Anagrafe tributaria, elaborato dall'Agenzia per superare le criticità rappresentate in passato (v. Relazione 2016, p. 39 s.), e ha invitato la stessa a implementare le misure prospettate, secondo la tempistica indicata, fornendo, di volta in volta, riscontro all'Autorità.

Il Garante ha inoltre rilevato e segnalato all'Agenzia delle entrate ulteriori gravi criticità, anche relative all'attività di vigilanza, quale titolare del trattamento, nei confronti di Sogei s.p.a., al fine di adottare tempestivamente le misure necessarie a porvi rimedio. In particolare, sono state riscontrate alcune vulnerabilità del sito istituzionale dell'Agenzia che, pur tenendo conto delle esigenze di continuità operativa e delle misure di *intrusion prevention* messe in atto con appositi strumenti tecnologici da Sogei, sono state risolte con eccessivo ritardo, anche in considerazione della

capacità tecnica del gestore, a cui appare ragionevole richiedere i più elevati livelli di sicurezza informatica, allo stato dell'arte, per i sistemi informativi strategici della p.a.

L'ulteriore problematica rilevata ha riguardato l'utilizzo del semplice protocollo FTP (*file transfer protocol*) per lo scambio automatizzato di flussi di dati con oltre duecento soggetti esterni senza la cifratura del canale di trasmissione dei dati scambiati tra *client* e *server* e, significativamente, dei dati di autenticazione informatica (*username* e *password* sono trasmessi in chiaro), determinando così una rilevante vulnerabilità agli attacchi informatici dei sistemi che lo utilizzano, con l'esposizione dell'infrastruttura al rischio informatico della compromissione delle credenziali di autenticazione utilizzate, peraltro già in tempi risalenti evidenziata dal Garante (provv. 18 settembre 2008, doc. web n. 1549548). L'analisi del rischio posta alla base di tale scelta tecnica, infatti, è stata incentrata esclusivamente sulla tipologia dei dati scambiati, trascurando le ricadute in termini di integrità e disponibilità dei dati nonché di sicurezza dei sistemi coinvolti (nota del Presidente 17 febbraio 2017, doc. web n. 6955457).

Sperimentazione di una procedura di selezione dei contribuenti

Su istanza dell'Agenzia delle entrate, previa istruttoria esplicata anche attraverso specifici accertamenti ispettivi, sono state ritenute idonee le misure e gli accorgimenti in materia di protezione dati previsti nell'ambito della sperimentazione di una procedura di selezione dei contribuenti basata sull'utilizzo delle informazioni fornite dall'Archivio dei rapporti finanziari e degli elementi presenti nell'Anagrafe tributaria per l'individuazione dei profili di evasione rilevanti. Tale procedura, relativa ad un ristretto campione di contribuenti, prevede una prima fase realizzata a livello centrale, di selezione del campione di contribuenti sulla base dell'indicatore di rischio oggetto di sperimentazione, individuando con l'elaborazione automatizzata incongruenze tra le somme a disposizione del contribuente e i redditi e le spese sostenute; una seconda fase operativa, svolta a cura delle sedi territoriali sulla base di specifiche istruzioni, riguarda la verifica dei dati e l'eventuale convocazione dei contribuenti. Le misure e gli accorgimenti individuati hanno riguardato, in particolare, la qualità dei dati utilizzati e la logica applicata ai trattamenti automatizzati effettuati nonché le garanzie per gli interessati. Inoltre, il Garante ha prescritto la trasmissione, non appena disponibili, delle risultanze della predetta sperimentazione, ai fini della valutazione in concreto dell'idoneità delle procedure e delle cautele adottate in vista degli ulteriori utilizzi del modello di analisi sperimentato (provv. 20 luglio 2017, n. 321, doc. web n. 6843736).

Dichiarazione dei redditi precompilata

Nell'ambito del percorso di approvazione della normativa di attuazione della cd. dichiarazione precompilata da parte del Mef e dell'Agenzia delle entrate, anche nel 2017 il Garante ha espresso numerosi pareri.

In primo luogo, a seguito di interventi normativi che hanno ampliato il novero delle informazioni da comunicare all'Agenzia delle entrate ai fini della predisposizione della dichiarazione precompilata, il Garante si è espresso favorevolmente su due schemi di provvedimento del Direttore dell'Agenzia delle entrate regolante la comunicazione, all'Anagrafe tributaria, dei dati relativi ai rimborsi delle spese universitarie ai sensi dell'art. 1, decreto del Ministro dell'economia e delle finanze 1° dicembre 2016 e dei dati relativi agli interventi di recupero del patrimonio edilizio e di riqualificazione energetica effettuati su parti comuni di edifici residenziali ai sensi dell'art. 2, decreto del Ministro dell'economia e delle finanze 1° dicembre 2016 (parere 19 gennaio 2017, n. 12, doc. web n. 6064930).

Nella medesima data il Garante ha altresì esaminato cinque schemi di provvedimento del Direttore dell'Agenzia delle entrate, integrativi di rispettivi precedenti provvedimenti, che disciplinano la comunicazione all'Anagrafe tributaria di informazioni per l'elaborazione della dichiarazione dei redditi precompilata, in materia

di contratti e premi assicurativi, interessi passivi per contratti di mutuo, spese sanitarie rimborsate, spese universitarie, contributi versati alle forme pensionistiche complementari; al riguardo le modifiche hanno riguardato esclusivamente le tipologie di informazioni da comunicare, senza modificare i canali di trasmissione e le relative misure di sicurezza (parere 19 gennaio 2017, n. 11, doc. web n. 6064866).

Successivamente, il Garante si è espresso sullo schema del nuovo provvedimento del Direttore dell'Agenzia sulle modalità di accesso alla dichiarazione precompilata da parte del contribuente e degli altri soggetti autorizzati che, nel confermare le modalità tecniche già disciplinate nel precedente provvedimento del 2016, tiene conto dell'incremento dei dati resi disponibili ai contribuenti per la dichiarazione 730 precompilata a partire dall'anno 2017 e delle problematiche evidenziate dal Garante nell'apposito tavolo di lavoro istituito per valutare la sicurezza dei trattamenti di dati personali, con particolare riferimento all'accesso da parte dei Caf (parere 17 marzo 2017, n. 163, doc. web n. 6378475).

Il Garante ha altresì espresso parere favorevole sullo schema di documento del Mef recante funzionalità telematiche rese disponibili dal Sistema tessera sanitaria ai fini della consultazione delle spese sanitarie da parte della collettività, che integra il documento tecnico regolante le modalità di consultazione dei dati di spesa sanitaria previste dall'art. 3-*bis*, d.lgs. n. 175/2014. In particolare, le osservazioni fornite dall'Autorità hanno riguardato le specifiche tecniche e le modalità operative delle procedure di accesso ai dati di spesa sanitaria da parte del pubblico (parere 5 luglio 2017, n. 300, doc. web n. 6843865).

Il Garante si è infine pronunciato favorevolmente sulla fornitura all'Agenzia, da parte della Ragioneria generale dello Stato-Ispettorato generale per la spesa sociale, dell'elenco dei contribuenti che hanno esercitato l'opposizione all'utilizzo delle spese sanitarie, per evitare la possibilità che, nella dichiarazione precompilata di tali soggetti, possano confluire, con altro flusso, i dati dei rimborsi delle spese sostenute comunicati dagli enti esterni. Tali elenchi saranno trasferiti, tramite appositi *file* criptati, tra le strutture di Sogei che seguono, rispettivamente, le attività del Sistema tessera sanitaria e della dichiarazione precompilata, senza alcun trattamento diretto dei dati da parte dell'Agenzia delle entrate (nota 12 aprile 2017).

FATCA

Il Garante si è espresso su un provvedimento dell'Agenzia delle entrate relativo all'attuazione della normativa in materia di scambio automatico obbligatorio di informazioni nel settore fiscale (Crs); nel disciplinare le modalità di comunicazione dei dati, lo stesso prevede che le Istituzioni finanziarie italiane, anche avvalendosi di fornitori terzi di servizi, trasmettano i *file* contenenti i dati per l'interscambio utilizzando l'infrastruttura informatica denominata Sid (sistema di interscambio dati), già oggetto di specifiche prescrizioni del Garante volte ad individuare le misure e gli accorgimenti idonei al fine di ridurre al minimo i rischi di accessi non autorizzati o di trattamenti non consentiti (pareri 17 aprile 2012, n. 145; doc. web n. 1886775; 15 novembre 2012, n. 861, doc. web n. 2099774 e 31 gennaio 2013, n. 48, doc. web n. 2268436). L'Autorità ha espresso parere favorevole a condizione che siano disciplinate, nella sede ritenuta più opportuna, le modalità di trattamento delle informazioni raccolte dall'Agenzia e che, prima dell'avvio degli scambi automatici di informazioni, siano assicurate idonee garanzie in materia di protezione dei dati personali in conformità alle linee guida del Gruppo Art. 29, con particolare riferimento allo scambio di dati con Paesi terzi non oggetto di una decisione di adeguatezza della protezione dei dati personali della Commissione europea (parere 22 giugno 2017, n. 283, doc. web n. 6587145).

Mef

Il Garante si è espresso favorevolmente, ai sensi degli artt. 19, comma 2, e 39, del Codice, sul protocollo d'intesa tra il Mef e la Banca d'Italia per l'accesso tele-

matico e l'aggiornamento delle procedure di trasmissione di dati e informazioni contenuti nell'archivio informatizzato Simec (sistema monitoraggio euro-carte) dell'ufficio centrale antifrode dei mezzi di pagamento (ufficio VI-Ucamp). In particolare, il protocollo, a seguito dell'implementazione dell'archivio informatizzato Simec-area euro (già Sirfe) che ha previsto la trasmissione per via telematica all'Ucamp dei dati e delle informazioni sui casi di sospetta falsificazione dell'euro, è volto a introdurre le nuove modalità di comunicazione al Centro nazionale di analisi (Cna), presso Banca d'Italia, dei dati identificativi (dati anagrafici e recapiti) contenuti nei verbali di ritiro delle banconote sospette di falsità elaborati dai gestori del contante che, allo stato, sono invece, inviati al Cna a mezzo posta – unitamente alle banconote – dai gestori del contante. Il protocollo prevede anche l'inserimento automatico in Simec-area euro, da parte del Cna, degli esiti degli accertamenti svolti sulle banconote inviate dai gestori del contante che allo stato, invece, sono comunicati al Mef, al fine di riconciliare i predetti esiti con le informazioni fornite dai gestori del contante ed avviare uno scambio di dati tra il Mef e la Banca d'Italia finalizzato a garantire l'allineamento tra i sistemi Simec-area euro e Faldan (procedura falsi e danneggiati utilizzata dalla Banca) delle anagrafiche degli enti segnalanti (tra i quali possono rilevare dati personali in caso, ad es., di ditte individuali) non espressamente previsto da norma di legge o regolamento (parere 26 ottobre 2017, n. 435, doc. web n. 7273446).

Equitalia

Il Garante ha fornito un positivo riscontro sul protocollo di intesa, trasmesso ai sensi dell'art. 39, comma 2, del Codice, tra l'Agenzia delle entrate ed Equitalia s.p.a. al fine di dare attuazione all'art. 6, d.l. 22 ottobre 2016, n. 193, convertito con modificazioni dalla legge 1° dicembre 2016, n. 225, che ha introdotto la possibilità per i contribuenti di definire, in via agevolata, i carichi affidati agli agenti della riscossione. Attraverso il protocollo è stato consentito ai singoli interessati di accedere agevolmente alle informazioni sulla propria posizione debitoria verso Equitalia s.p.a. anche presso gli sportelli dell'Agenzia delle entrate o presso gli intermediari abilitati ai servizi telematici dell'Agenzia (nota 9 marzo 2017).

4.6. *La videosorveglianza in ambito pubblico*

Come già avvenuto in passato, il Garante è stato più volte chiamato a pronunciarsi in merito al trattamento di dati personali effettuato tramite sistemi di videosorveglianza in ambito pubblico. Tra i molteplici chiarimenti forniti, si segnalano quelli riguardanti le modalità di istallazione di impianti di videosorveglianza all'interno di centri abitati da parte dei comuni, in particolare in relazione agli impianti volti a contrastare l'abbandono incontrollato di rifiuti urbani attraverso i dispositivi denominati foto trappola (predisposti per rilevare delle immagini solo al verificarsi di condizioni predefinite). In proposito, è stato evidenziato che, a fronte dell'inefficacia di strumenti e sistemi di controllo alternativi, l'utilizzo di impianti di videosorveglianza risulta lecito anche per accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose nonché per monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (cfr. art. 13, l. 24 novembre 1981, n. 689 e punto 5.2, provv. 8 aprile 2010, doc. web n. 1712680). In questo ambito, un caso oggetto di segnalazione ha riguardato la presunta assenza di informativa rispetto ad un sistema di videosorveglianza collocato in un piazzale per controllare il regolare deposito dei rifiuti. Dalle informazioni acquisite, è risultato che il cartello recante l'informativa era stato collocato, in modo ben visibile anche

durante le ore notturne, a qualche decina di metri dall'area interessata dal raggio di azione della telecamere e pertanto il trattamento dei dati è stato ritenuto conforme alla disciplina in materia di protezione dei dati personali. È stato in particolare evidenziato che il supporto con l'informativa non deve essere necessariamente collocato a stretto contatto con gli impianti, ma nelle sue immediate vicinanze e comunque, prima dell'area interessata dalle riprese (cfr. punto 3.1. del citato provvedimento generale). In casi come quello descritto, anche quando il sistema di videosorveglianza è impiegato per la prevenzione dei reati ambientali (riconducibile all'ambito applicativo dell'art. 53 del Codice e per ciò stesso quindi esonerato dall'obbligo di informativa), si è ritenuto di raccomandare agli enti pubblici di collocare comunque i cartelli contenenti l'informativa perché rendere palese l'utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una ulteriore ed efficace funzione di deterrenza, oltre quelle specificamente perseguite (cfr. punto 3.1.2. del provvedimento generale) (nota 18 gennaio 2017).

Scuole

Specifiche istruttorie sono state avviate anche con riferimento all'impiego di sistemi di videosorveglianza in ambito scolastico. In tale ambito l'Ufficio oltre a richiamare le specifiche indicazioni già fornite dall'Autorità sull'informativa (cfr. punti 3.1. e 4.6. del citato provvedimento; artt. 13 e 161 del Codice), ha spesso ribadito 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 assicurarne l'armonico sviluppo della personalità, il processo di maturazione ed il diritto all'educazione. È stato inoltre evidenziato che può risultare ammissibile l'utilizzo di sistemi di videosorveglianza soltanto 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 ed attivando gli impianti negli orari di chiusura degli istituti (punto 4.3.1) nonché chiarendo 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 (nota 27 giugno 2017).

Luoghi di cura

Con riguardo alla videosorveglianza presso luoghi di cura, merita una menzione la richiesta del responsabile di una residenza sanitaria per l'allungamento – sino a trenta giorni – dei tempi di conservazione delle immagini registrate presso taluni locali motivata sulla base del fatto che la rilevazione di comportamenti anomali o maltrattamenti, e la conseguente denuncia, richiedono di massima tempi più lunghi rispetto ai previsti sette giorni in ragione della peculiare condizione di fragilità dei soggetti assistiti.

L'Autorità ha, in primo luogo, fornito indicazioni in ordine alla procedura da seguire per la richiesta di prolungamento dei tempi di conservazione delle immagini registrate oltre il previsto termine di sette giorni, segnalando la necessità di una verifica preliminare del Garante ed evidenziando al contempo la necessità che, nel rispetto del principio di proporzionalità, la richiesta in parola sia adeguatamente motivata sulla base di una specifica esigenza di sicurezza, riferita a concrete situazioni di rischio (punti 3.2.1. e 3.4. del cit. provv. generale dell'8 aprile 2010).

Il Garante ha poi chiarito che la dichiarata finalità di contrasto alle condotte di maltrattamento nei confronti degli ospiti della struttura non è, in assenza di una specifica regolamentazione, compatibile con le finalità proprie della residenza sanitaria, essendo invece propria dei trattamenti a scopo di prevenzione e repressione dei reati di competenza delle Forze di polizia. Su tale tematica sono state richiamate le specifiche iniziative legislative portate all'attenzione del Parlamento, sulle quali l'Autorità aveva già espresso la propria posizione in occasione delle audizioni del presidente Soro, in relazione alle proposte di legge recanti norme in materia di videosorveglian-

za negli asili nido e nelle scuole dell'infanzia nonché nelle strutture socio-assistenziali per anziani, disabili e minori in situazione di disagio, presso le Commissioni riunite I e XI della Camera dei deputati (27 luglio 2016, doc. web n. 5301830) e presso la 11ª Commissione permanente (lavoro, previdenza sociale) del Senato della Repubblica (22 novembre 2016, doc. web n. 5696272) (note 20 aprile e 10 luglio 2017).

L'Autorità è stata chiamata ad esprimersi nell'ambito di una richiesta di verifica preliminare presentata da una azienda ospedaliera per il prolungamento, fino a venti giorni, della durata del periodo di conservazione delle immagini raccolte dai sistemi di videosorveglianza.

Esaminate le caratteristiche del sistema, il Garante ha condiviso la manifestata esigenza di sicurezza e l'opportunità di ammettere una conservazione delle immagini registrate per un periodo superiore alla settimana al fine di tutelare gli interessi degli utenti, dei terzi e dei dipendenti, considerati gli specifici eventi verificatisi (furti, aggressioni e effrazioni, avvenuti in danno dell'azienda e del personale). Il Garante ha, in ogni caso, richiamato l'attenzione dell'azienda ospedaliera sulle prescrizioni relative alle misure di sicurezza, sulle garanzie relative al trattamento di dati personali in ambito lavorativo e presso gli ospedali (cfr. punti 3.3.1, 4.1. e 4.2. del citato provvedimento generale; artt. 31-36, del Codice e all. B al Codice; artt. 114 del Codice e 4, l. 20 maggio 1970, n. 300, recante il cd. Statuto dei lavoratori) nonché sulla necessità di aggiornare la bozza di regolamento sull'utilizzo in ambito aziendale di sistemi di videosorveglianza trasmesso all'Autorità (provv. 31 maggio 2017, n. 256, doc. web n. 6630601).

Videoriprese di privati per finalità di tutela dei diritti e di polizia

Un'amministrazione comunale ha chiesto all'Autorità un parere in merito alla produzione in giudizio delle videoriprese consegnate ed effettuate da privati attraverso l'installazione di dispositivi posti all'esterno della propria abitazione al fine di sorvegliare il proprio domicilio. In sostanza il comune, non avendo la disponibilità, per ragioni economiche, di un proprio sistema di videosorveglianza, ha chiesto di poter acquisire ed allegare agli atti di indagine le videoriprese effettuate da privati per fini personali e che ritraggono autori di illeciti sorpresi nell'atto di abbandonare o incendiare rifiuti. Ciò in quanto, secondo l'orientamento della Suprema Corte (sent. n. 22093/2015) "le videoriprese eseguite da privati che importano luoghi di privata dimora liberamente visibili dall'esterno senza particolari accorgimenti" costituirebbero prova atipica ai sensi dell'art. 189 c.p.p., "pienamente utilizzabili senza l'autorizzazione dell'autorità giudiziaria".

In proposito sono stati richiamati, in applicazione del provvedimento generale dell'8 aprile 2010 (doc. web n. 1712680), i limiti relativi all'utilizzo di sistemi di videosorveglianza per fini esclusivamente personali in presenza di concrete situazioni che ne giustifichino l'installazione (a protezione delle persone, della proprietà o del patrimonio aziendale), anche alla luce della sentenza della Corte di Giustizia (quarta sezione, C-212/13, 11 dicembre 2014) secondo cui l'utilizzo di un sistema di videocamera, installato da una persona fisica sulla propria abitazione per proteggere i beni, la salute e la vita dei proprietari dell'abitazione, se in grado di riprendere anche lo spazio pubblico, non costituisce più un trattamento dei dati effettuato per l'esercizio di attività a carattere esclusivamente personale e, pertanto, deve avvenire nel rispetto della normativa in materia di protezione dei dati personali. Sulla base di tali considerazioni, l'Autorità ha affermato che nella fattispecie in esame le videoriprese sono lecite se le telecamere sono orientate in modo da riprendere solo gli spazi di proprietà esclusiva dei privati e non anche lo spazio pubblico, né *a fortiori* gli spazi di proprietà di terzi quandanche esposti alla pubblica osservazione. In questi ultimi casi, infatti, tali dati, in quanto acquisiti illecitamente, non sarebbero utilizzabili (art. 11, comma 2, del Codice).

Diverso il caso di utilizzo di impianti di videosorveglianza finalizzati alla tutela della sicurezza urbana, acquistati da soggetti privati, ma utilizzati esclusivamente e sotto la responsabilità di Forze di polizia. In un caso analogo, infatti, l'Ufficio ha ritenuto lecito l'utilizzo, da parte di un comune, di videoriprese effettuate attraverso telecamere acquistate da privati, ma gestite esclusivamente da agenti di Polizia locale, che rivestono la qualifica di agenti di pubblica sicurezza. In tale circostanza, infatti, poiché ai sensi dell'art. 6, d.l. 23 febbraio 2009, n. 11, convertito con l. 23 aprile 2009, n. 38, "per la tutela della sicurezza urbana, i comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico", l'eventuale assunzione degli oneri finanziari per l'acquisto e la manutenzione degli impianti di videosorveglianza da parte di privati sarebbe del tutto indifferente per quanto attiene alla normativa in materia di protezione dei dati personali. Ciò a condizione che il privato acquirente sia escluso da qualsiasi utilizzo e accesso al sistema di videosorveglianza, dovendo il comune, titolare del trattamento, informare il privato in ordine al divieto assoluto di intromissione nel sistema informatico ed alle gravi conseguenze in caso di violazione del divieto (nota 17 marzo 2017).

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

Eventi sismici

In relazione agli eventi sismici che hanno ripetutamente colpito il territorio delle Regioni Lazio, Marche, Umbria e Abruzzo nel 2016, su richiesta del Dipartimento della protezione civile, il Garante ha individuato, ai sensi dell'art. 13, comma 3, del Codice, le modalità semplificate con le quali il Dipartimento della protezione civile, le regioni e i comuni interessati avrebbero potuto rendere l'informativa in qualità di titolari o contitolari dei trattamenti dei dati personali raccolti nell'ambito della gestione dello stato di emergenza ed effettuati nel periodo successivo alla scadenza dello stato di emergenza.

Al riguardo, lo stato di emergenza per gli eventi sismici che hanno interessato l'Italia centrale, è stato dichiarato, ai sensi dell'art. 5, l. 24 febbraio 1992, n. 225, e prorogato fino al 20 agosto 2017, con le delibere del Consiglio dei ministri 25 agosto 2016 e 10 febbraio 2017. Il capo del Dipartimento della protezione civile, con ordinanza 28 agosto 2016, n. 389, al fine di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, anche sensibili e giudiziari, nei territori interessati, ha disposto una disciplina derogatoria ad alcune disposizioni del Codice, pur nel rispetto dei principi in esso sanciti, per consentire lo svolgimento degli adempimenti fissati dalla normativa di settore. Tenuto conto dei preminenti interessi salvaguardati con le operazioni di soccorso, in relazione ai trattamenti di dati personali effettuati dai soggetti istituzionali coinvolti, con la predetta ordinanza è stato differito l'adempimento degli obblighi di informativa fino al termine dello stato di emergenza. È stato altresì previsto che, alla scadenza, la predetta informativa sarebbe stata resa secondo le modalità semplificate individuate con provvedimento del Garante ai sensi dell'art. 13, comma 3, del Codice.

Con provvedimento 26 luglio 2017, n. 342 (doc. web n. 6820964), pertanto, la pubblicazione dell'informativa in apposita sezione dei siti web istituzionali del Dipartimento della protezione civile, delle regioni e dei comuni degli ambiti territoriali oggetto delle dichiarazioni dello stato di emergenza, è stata ritenuta adeguata ad assicurare la conoscenza necessaria per la tutela dei diritti previsti dalla normativa in materia di protezione dei dati personali.

Obblighi vaccinali

Interpellato da numerose regioni, istituti scolastici e da singoli interessati, in relazione agli aspetti di protezione dei dati personali connessi ai nuovi obblighi vaccinali

previsti dall'art. 1, d.l. n. 73/2017 per i minori di età compresa tra zero e sedici anni (come rappresentato nel par. 2.1.1), il Garante si è pronunciato al riguardo con il provv. 1° settembre 2017, n. 365 (doc. web n. 6765917), oggetto di più analitico esame al par. 5.2.1.

Fiscalità dell'auto

È stata inoltre conclusa l'istruttoria relativa a un progetto sperimentale sulla fiscalità dell'auto, sottoposto dalla Città metropolitana di Roma Capitale nel 2016. Il progetto prevedeva l'invio di una nota di cortesia agli automobilisti residenti nel territorio per segnalare l'assenza di copertura assicurativa obbligatoria e le possibili conseguenze (art. 193, d.lgs. n. 285/1992; art. 13, comma 3, l. n. 689/1981) ed era finalizzato a contrastare il fenomeno dell'evasione dell'obbligo assicurativo, anche in relazione al profilo di evasione dell'imposta provinciale sulle assicurazioni (art. 60, d.lgs. n. 446/1997; artt. 17, d.lgs. n. 68/2011), principale entrata tributaria delle Città metropolitane a seguito del subentro alle province (art. 1, comma 47, l. n. 56/2014).

Il Garante ha ritenuto che tale iniziativa, pur se meritoria, non rientrava tra le finalità istituzionali dell'ente e che, pertanto, il relativo trattamento di dati personali non poteva considerarsi conforme alla disciplina del Codice (art. 18). Ha inoltre osservato che il fenomeno dell'evasione dell'obbligo assicurativo interessa unitariamente l'intero territorio nazionale, così come le conseguenze negative sulle vittime di sinistri stradali non sono necessariamente correlate al territorio di residenza del proprietario del veicolo. Per contrastare il fenomeno, infatti, il legislatore ha istituito la banca dati dei contrassegni assicurativi e ha demandato il risarcimento dei danni provocati da veicoli privi di assicurazione al Fondo di garanzia per le vittime della strada, in un sistema che vede coinvolti, a vario titolo, molteplici attori istituzionali (Ministeri delle infrastrutture e dei trasporti, dello sviluppo economico, Ivass, Consap, Ania, imprese assicurative).

A seguito delle osservazioni formulate dall'Ufficio, la Città metropolitana di Roma Capitale, ha accolto l'invito a coinvolgere nell'iniziativa gli altri attori istituzionali competenti. In particolare, riconoscendo al Ministero delle infrastrutture e dei trasporti un ruolo centrale nel contrasto al fenomeno dell'evasione dell'obbligo assicurativo per la responsabilità civile, la Città metropolitana ha promosso l'iniziativa presso il predetto Ministero, proponendosi per una prima sperimentazione su base locale, da estendere all'ambito nazionale (nota 9 gennaio 2017).

Smarrimento supporti elettronici

Un comune ha segnalato alcune criticità in merito all'applicazione della disciplina civilistica concernente la consegna di dispositivi elettronici al soggetto che li ha rinvenuti, integrate le condizioni previste dal codice civile (artt. 927-929 c.c.). In particolare, è stata evidenziata la potenziale grave compromissione della sfera privata derivante dalla materiale possibilità di accedere ai dati registrati su tali dispositivi (fotografie, video, rubriche telefoniche, corrispondenza, etc.) anche nel caso in cui, prima della consegna al rinvenitore, si provveda, senza adottare cautele specifiche, alla loro cancellazione; ciò anche in relazione alla prassi in uso presso altri enti locali, consistente nella acquisizione della mera dichiarazione di non utilizzare tali dati resa dalla persona a cui l'oggetto viene consegnato.

Ritenendo condivisibili le preoccupazioni rappresentate dall'ente, l'Ufficio ha indicato al comune alcune misure tecniche da adottare prima della consegna al rinvenitore di tali dispositivi. Ipotizzando che nella maggior parte dei casi gli oggetti smarriti siano apparati di piccole dimensioni compresi nella categoria dei dispositivi portatili (cellulari, *smartphone, tablet, computer* portatili etc.), è stato suggerito di prevedere, prima della consegna del bene al ritrovatore, la rimozione delle schede eventualmente presenti nel dispositivo, di effettuare il cd. *reset* dello stesso, portandolo ad una installazione pari al nuovo, priva di dati e di qualsiasi impostazione rife-

ribile all'utente precedente (ivi compresa la disabilitazione delle connessioni di rete eventualmente impostate e di ulteriori impostazioni personalizzate); qualora praticabile, la sovrascrittura irreversibile di tutte le memorie del dispositivo attraverso programmi software *ad hoc* che, anche in caso di supporti apparentemente privi di dati ed impostazioni personalizzate, renda irrecuperabili i dati e le informazioni di qualsiasi tipo riferibili al precedente proprietario; la rimozione delle schede Sim eventualmente presenti nel dispositivo. Infine, nel caso in cui, per qualsiasi ragione, debba disporsi la distruzione di dispositivi elettronici o, comunque, di supporti contenenti dati personali, al fine di evitare qualsiasi rilevamento ed utilizzo dei dati in essi contenuti, sono state richiamate le prescrizioni contenute nel provvedimento 13 ottobre 2008 (doc. web n. 1571514) (nota 14 febbraio 2017).

Notificazione degli atti giudiziari

In materia di notificazione degli atti giudiziari ai soggetti interessati, è stato segnalato che in risposta a un'istanza in autotutela presentata in relazione alla comunicazione tardiva di un atto, un comune, ritenendo infondata la richiesta, aveva trasmesso al segnalante l'elenco dei soggetti cui erano stati inviati gli atti, tra i quali figurava quello dell'interessato e di altre 67 persone, unitamente agli indirizzi di notifica. Al riguardo l'Ufficio ha evidenziato che il trattamento dei dati personali da parte dei soggetti pubblici è consentito soltanto "per lo svolgimento delle funzioni istituzionali" e che la comunicazione di dati personali a privati è ammessa unicamente quando è prevista da una norma di legge o di regolamento, nel rispetto dei principi di pertinenza e non eccedenza rispetto alle finalità perseguite (artt. 11, comma 1, lett. *d*), 18 e 19, comma 3, del Codice). Nel caso di specie, trasmettendo integralmente il prospetto contenente l'elenco degli avvisi di accertamento notificati a mezzo posta dal comune, senza provvedere ad oscurare i dati personali (nome, cognome e indirizzo) relativi ai soggetti diversi dal segnalante, il comune ha effettuato una comunicazione a privati di dati personali non sorretta da idonea base normativa e non necessaria in relazione alla dichiarata predetta finalità di dimostrare all'interessato l'avvenuta notifica dell'atto, in violazione degli artt. 19, comma 3, e 11, comma 1, lett. *d*), del Codice, per la quale è stato avviato il relativo procedimento sanzionatorio (nota 7 luglio 2017).

Diffusione di dati sulla salute nel corso del consiglio comunale

In un altro caso, il Garante è intervenuto, dichiarando illecito il trattamento effettuato da un comune a seguito di una segnalazione concernente la diffusione, durante la seduta di un consiglio comunale, di informazioni, anche sensibili, relative a una dipendente. Nella fattispecie esaminata, oltre alla lettura di alcuni stralci di una nota nella quale erano riportati, tra l'altro, dati relativi alla diagnosi e alla prognosi di un accertamento del pronto soccorso e, a periodi di assenza per malattia e infortunio, era stato anche pubblicato il verbale della seduta sul sito istituzionale del comune. Al riguardo, è stato evidenziato che in relazione al trattamento dei dati personali effettuato da soggetti pubblici, specifiche disposizioni prevedono che i "dati idonei a rivelare lo stato di salute non possono essere diffusi", con la conseguenza che risulta vietata la diffusione di qualsiasi dato da cui possa desumersi 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 (art. 22, comma 8, nonché art. 65, comma 5, del Codice; provv. 15 maggio 2014, n. 243, doc. web n. 3134436). Pertanto, pur prendendo atto del fatto che il verbale non era più rinvenibile sul sito del comune nonché della circostanza che la vicenda trattata durante il consiglio comunale aveva avuto una certa risonanza mediatica sulla stampa e sui *social network*, anche prima della seduta consiliare, l'Ufficio ha ritenuto il trattamento in parola non conforme all'art. 22, comma 8, del Codice, e ha avviato il relativo procedimento sanzionatorio (nota 18 maggio 2017).

4.8. *La previdenza e l'assistenza sociale*

Il Garante si è espresso sulla normativa attuativa dell'art. 1, comma 175, l. 11 dicembre 2016, n. 232, in materia di anticipo finanziario a garanzia pensionistica (Ape). In particolare, con parere 26 luglio 2017, n. 335 (doc. web n. 6820552), sono state fornite indicazioni sul contenuto dell'informativa da fornire agli interessati, sui ruoli assunti nel trattamento dei dati e sulle misure necessarie ad assicurare la minimizzazione dei dati nella trasmissione dei messaggi di posta elettronica. Successivamente, con provvedimento 29 dicembre 2017, n. 567 (doc. web n. 7509712), il Garante ha fornito il proprio parere sugli schemi dell'Accordo quadro per l'Ape e dell'Accordo quadro per la polizza assicurativa obbligatoria per il rischio di premorienza da stipularsi tra il Ministro dell'economia e delle finanze e il Ministro del lavoro e delle politiche sociali, l'Associazione bancaria italiana e l'Associazione nazionale fra le imprese assicuratrici per definire, in particolare, le specifiche tecniche e di sicurezza dei flussi informativi tra Inps, istituti finanziatori e imprese assicurative. Nel parere è stato previsto di sottoporre all'esame del Garante anche il documento tecnico, elaborato dall'Inps, ove saranno definite l'infrastruttura applicativa e le specifiche tecniche e di sicurezza con conseguente possibile revisione della modulistica di adesione. È risultato inoltre necessario richiedere una precisazione del ruolo assunto da parte dell'Associazione nazionale fra le imprese assicuratrici (Ania) nel trattamento dei dati personali nell'ipotesi in cui essa stessa funga da collegamento tra l'Inps e le imprese assicuratrici, prevista dell'Accordo quadro assicurativo (parere 29 dicembre 2017, n. 567, doc. web n. 7509712).

5 La sanità e i dati genetici

5.1. *I trattamenti per fini di cura*

Numerose sono state le istruttorie definite dal Garante in materia di trattamento dei dati personali in ambito sanitario. In un caso, l'Autorità è venuta a conoscenza di iniziative intraprese da alcuni dipartimenti ospedalieri di emergenza relative alla prevenzione e cura della violenza domestica e, più in generale, di quella perpetrata nei confronti delle donne. In particolare, è stata riscontrata l'intenzione di redigere, presso il pronto soccorso, apposita documentazione, anche fotografica, in merito alle specifiche lesioni subite dalla vittima a seguito della violenza. Al riguardo, l'Ufficio ha inviato una comunicazione alla regione interessata e alla Presidenza del Consiglio dei ministri evidenziando che la normativa vigente prevede che, con decreto del Presidente del Consiglio dei ministri, siano definite, a livello nazionale, le linee guida volte a rendere operativo il percorso di tutela delle vittime di violenza (Convenzione del Consiglio d'Europa sulla prevenzione e la lotta alla violenza contro le donne e la violenza domestica dell'11 maggio 2011; d.l. 14 agosto 2013, n. 93, convertito in legge 15 ottobre 2013, n. 119; art. 1, comma 790, l. 28 dicembre 2015, n. 208). È stato quindi evidenziato che le iniziative poste in essere a livello locale devono essere conformi al citato quadro normativo al fine di evitare, da un lato, approcci disarmonici sul territorio nazionale e, dall'altro, l'individuazione di modalità operative non corrette rispetto alla normativa in materia di protezione dei dati personali, in particolare sotto il profilo di un'adeguata e preventiva valutazione del rischio (nota 31 maggio 2017).

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

Merita evidenziare alcune specifiche istruttorie avviate a seguito di segnalazioni circa illecite comunicazioni di dati sensibili. In tale ambito, l'Ufficio ha accertato che un centro di riabilitazione, in assenza di idonea base normativa, aveva comunicato ad alcune Istituzioni regionali dati idonei a rivelare lo stato di salute di più di 80 pazienti in lista di attesa. L'Ufficio ha al riguardo evidenziato che la dichiarata finalità perseguita dal centro di rappresentare agli organi di governo sanitario il fabbisogno di assistenza riabilitativa sul territorio poteva essere utilmente raggiunta anche senza indicare i nominativi degli assistiti e che la manifestazione di volontà espressa dai pazienti per tale comunicazione non poteva ritenersi presupposto idoneo, in quanto non effettuata nell'ambito delle finalità di diagnosi, cura e riabilitazione degli interessati, bensì per finalità amministrative (nota 15 febbraio 2017).

In altri due casi l'Ufficio ha accertato l'avvenuta comunicazione, da parte di due strutture sanitarie, di dati personali idonei a rivelare lo stato di salute di un paziente al suo datore di lavoro. Nel rilevare l'illecito trattamento e avviare il connesso procedimento sanzionatorio, è stato ribadito che la disciplina in materia di protezione dei dati personali prevede che gli esercenti le professioni sanitarie e gli organismi sanitari possano, nel perseguimento delle finalità di cura della salute, comunicare al solo interessato le informazioni relative al suo stato di salute (art. 84 del Codice). In assenza del consenso dell'interessato, la struttura sanitaria può comunicare i dati

idonei a rivelare lo stato di salute solo nei limiti previsti dalle norme vigenti (artt. 20 e ss. e 75 e ss. del Codice) (note 15 febbraio e 6 marzo 2017).

Con specifico riguardo al trattamento di dati idonei a rivelare lo stato di salute dei lavoratori, è stato inoltre evidenziato che la sussistenza di specifici obblighi normativi nei riguardi del lavoratore, per consentire al datore di lavoro di verificare le sue reali condizioni di salute nelle forme di legge, giustifica che, per motivare l'assenza, venga fornita all'amministrazione di appartenenza apposita documentazione consistente in un certificato medico contenente la sola indicazione dell'inizio e della durata presunta dell'infermità (prognosi). In assenza di speciali disposizioni di natura normativa, che dispongano diversamente per specifiche figure professionali, il datore di lavoro pubblico non è pertanto legittimato a raccogliere certificazioni mediche contenenti anche l'indicazione della diagnosi (cfr. linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico: provv. 14 giugno 2007, n. 161, doc. web n. 1417809).

In più occasioni, strutture sanitarie territoriali hanno chiesto all'Autorità l'autorizzazione a fornire agli interessati un'informativa semplificata in relazione al mutato assetto del sistema sanitario regionale. In uno dei casi affrontati è stato chiesto al Garante di pronunciarsi in seguito all'adozione di una procedura di cessione di un ramo di azienda che ha visto coinvolte tre strutture sanitarie con contestuale trasferimento delle attività di diagnostica di laboratorio dalle strutture cedenti a quella del cessionario. Il Garante ha accolto la richiesta in considerazione del fatto che il trattamento dei dati personali dei pazienti afferenti alle attività diagnostiche di laboratorio cedute sarebbe rimasto invariato rispetto a quello effettuato dai cedenti, sia in termini di finalità, che di modalità del trattamento. Tenuto conto che tale cessione si inseriva in un più ampio processo di riforma del servizio sanitario regionale, reso noto dai principali mezzi di informazione locali, e che sarebbe stato troppo oneroso, per le aziende coinvolte, rendere un'informativa individuale agli oltre 200.000 pazienti coinvolti, l'Autorità ha ritenuto ragionevole che fossero forniti agli interessati i necessari aggiornamenti delle informative originariamente rese dalle aziende sia attraverso il sito web delle stesse, sia mediante comunicazione individualizzata agli interessati alla prima occasione utile di contatto, anche successiva al completamento delle operazioni di cessione. Con specifico riferimento al consenso dei pazienti coinvolti dalla suddetta cessione, il Garante ha valutato che la raccolta con modalità ordinarie di una nuova manifestazione di volontà avrebbe comportato un impiego di mezzi manifestamente sproporzionati in termini di tempo, costi e oneri amministrativi e ha conseguentemente autorizzato la comunicazione dei dati dei pazienti e il successivo trattamento svolto per effetto della cessione del ramo d'azienda (provv. 19 gennaio 2017, n. 13, doc. web n. 6093240).

Sullo stesso tema, il Garante ha esonerato le aziende sanitarie delle Regioni Veneto e Toscana dall'obbligo di rendere una nuova informativa in forma individuale ai pazienti in sede di ridefinizione dell'assetto organizzativo delle aziende stesse. Per quanto riguarda la Regione Veneto, la richiesta era stata avanzata da due delle aziende Ulss che avevano incorporato altre Ulss per effetto della riorganizzazione prevista dalla legge regionale n. 19/2016. Il Garante, con provvedimento 31 maggio 2017, n. 255 (doc. web n. 6531135), in forza del Codice e dell'autorizzazione generale n. 2/2016, ha autorizzato le suddette aziende al trattamento dei dati sanitari dei pazienti afferenti alle aziende coinvolte dal processo di incorporazione, esclusivamente per le finalità di cura originariamente perseguite e salva la comunicazione agli interessati della nuova denominazione del titolare del trattamento in occasione della prima circostanza utile di contatto; nella medesima circostanza, nell'accogliere le istanze provenienti dalle stesse aziende Ulss di esonero dall'obbligo di rendere una

nuova informativa in forma individuale, è stato prescritto di aggiornare le informative originariamente rese con l'esonero dal rendere la nuova informativa in forma individuale a tutte le aziende Ulss della Regione Veneto coinvolte in procedure analoghe. Anche in questo caso, il Garante ha ritenuto che una nuova manifestazione del consenso dei pazienti avrebbe comportato un impiego di mezzi manifestamente sproporzionati in termini di tempo, costi e oneri amministrativi, posto che il trattamento rimane invariato rispetto a quello effettuato dalle aziende incorporate e che è interesse dei pazienti vedere garantita la conservazione dei dati che li riguardano – già raccolti e custoditi dalle strutture sanitarie incorporate – e preservata la prosecuzione del loro trattamento.

Similmente, per quanto concerne il caso della Regione Toscana, essendo state riunite le aziende Usl della Regione in tre macro unità in virtù della legge regionale n. 84/2015, il Garante ha esonerato l'azienda Usl richiedente dall'obbligo di rendere una nuova informativa in forma individualizzata (prescrivendo che la stessa venisse resa attraverso il proprio sito web e mediante comunicazione individualizzata agli interessati in occasione della prima circostanza utile di contatto) nonché prevedendo modalità semplificate per la raccolta del consenso; tali previsioni sono state estese anche alle altre due Usl della Regione (provv. 16 novembre 2017, n. 477, doc. web n. 7490004).

5.1.2. Il Fascicolo sanitario elettronico e il dossier *sanitario*

Anche nel 2017 l'Autorità ha partecipato attivamente ai lavori del tavolo tecnico di monitoraggio e indirizzo per l'attuazione delle disposizioni inerenti il Fascicolo sanitario elettronico (Fse), che vede la partecipazione degli organi centrali e regionali di governo sanitario (cfr. art. 26, d.P.C.M. n. 178/2015). Nell'ambito di tali lavori, sono stati forniti chiarimenti in merito all'applicazione delle disposizioni poste a tutela della riservatezza degli interessati, addivenendo a determinazioni congiunte in vista di sistemi uniformi e dialoganti sul territorio nazionale. In particolar modo, sono state fornite indicazioni circa la possibilità di ammettere che i consensi previsti per i trattamenti effettuati tramite il Fse siano manifestati da soggetti diversi dall'interessato, le modalità di accesso al Fse in caso di emergenza per l'interessato o per terzi/collettività e quelle per la cancellazione dei dati presenti sul Fse nonché per la manifestazione di volontà che deve esprimere il genitore per il Fse del minore (nota 21 febbraio 2017).

Riguardo alla possibilità di "delegare" terzi all'accesso al Fse nonché alla gestione di alcune delle operazioni interattive consentite all'interessato tramite il Fse, l'Autorità ha ritenuto che non vi siano elementi ostativi a che l'interessato, capace di intendere e di volere, deleghi un soggetto terzo a consultare il proprio Fse, analogamente a quanto già indicato con riferimento al ritiro dei referti (anche con modalità digitali) e, più in generale, di tutti i documenti contenenti dati sanitari che lo riguardano (cfr. provv. 13 marzo 2014, n. 120, doc. web n. 3041470; provv. 9 novembre 2005, doc. web n. 1191411). Tale delega può essere validamente resa sia attraverso le modalità ordinarie (delega tramite verifica da parte del titolare del trattamento dell'identità del soggetto incaricato attraverso l'esibizione di un documento di riconoscimento e la registrazione degli estremi dello stesso), che tramite idonee procedure informatiche che abbiano requisiti equivalenti, definendo anche le modalità per l'eventuale revoca della delega (nota 12 giugno 2017).

L'Autorità ha poi analizzato le iniziative sorte in ambito regionale che prevedono, secondo sistemi diversamente articolati, una notifica al medico di medicina generale/pediatra di libera scelta (MMG/PLS) circa la presenza di nuovi documenti consultabili attraverso il Fse (notifiche di aggiornamenti; notifiche di pubblicazione dei

dati). Al riguardo si è ritenuto che il suddetto servizio di notifica al MMG/PLS, indipendentemente dalle modalità di realizzazione dello stesso, non possa essere ricondotto ai servizi propri del Fse. Ciò non solo perché non è espressamente previsto dall'impianto normativo vigente, ma anche in quanto si configura come servizio ulteriore rispetto al Fse, strettamente connesso al rapporto medico-paziente (infatti i documenti sarebbero consultabili dal MMG/PLS anche senza accedere al Fse dell'assistito). Il Fse, infatti, non si configura come uno strumento mediante il quale il medico curante acquisisce nei propri sistemi informativi i documenti sanitari dell'assistito (effettuando così una duplicazione dei documenti indicizzati sul Fse). Al contrario, esso è uno strumento attraverso il quale tutti i medici che intervengono nel percorso di cura possono consultare i documenti sanitari riferibili all'interessato, che continuano però a permanere presso la struttura sanitaria che li ha generati (sistema di indicizzazione centrale dei documenti sanitari) (nota 12 giugno 2017).

Sono stati poi forniti elementi in merito alla cd. medicina di iniziativa che, allo stato, non risulta regolata nell'ordinamento nazionale. Al riguardo, l'Autorità, appreso che in diverse regioni, con specifico riferimento a alcune patologie croniche (es. diabete) o a determinate malattie oncologiche (tumore mammario), sono stati sviluppati, a livello regionale, strumenti informatici che, elaborando le informazioni derivanti dai documenti sanitari dell'assistito, mettono a disposizione dei MMG/PLS un profilo sanitario di rischio dell'assistito, indirizzando il medico a proporre allo stesso specifici accertamenti diagnostici in chiave di prevenzione, ha invitato il Ministero della salute a disciplinare la materia, anche in ragione dei significativi risvolti etici (diritto di non sapere). Nelle more dell'intervento del legislatore, il Garante ha ritenuto di evidenziare che l'adozione di tali sistemi determina la raccolta e l'elaborazione di dati sanitari al fine di realizzare, con riferimento a specifiche patologie, un profilo sanitario di rischio dell'interessato e configura quindi un trattamento autonomo rispetto a quello principale. Tale trattamento può quindi essere effettuato esclusivamente da esercenti le professioni sanitarie per finalità di prevenzione e sulla base di uno specifico consenso informato dell'interessato, nel rispetto dei principi indicati nell'Autorizzazione n. 2 del Garante (nota 12 giugno 2017).

Con riferimento all'emendamento di modifica della disciplina sul Fse dettata dalla legge di bilancio 2017, il Garante ha espresso il proprio parere sullo schema di decreto del Mef di concerto con il Ministero della salute, concernente le modalità tecniche e i servizi telematici resi disponibili all'infrastruttura nazionale per l'interoperabilità dei Fse (parere 26 luglio 2017, n. 339, doc. web n. 6930323). I principali aspetti affrontati dall'Autorità nel corso dell'elaborazione del decreto e del relativo parere hanno riguardato la necessità di analizzare la tipologia di dati e documenti che legittimamente sono conservati sul Sistema TS, al fine di individuare quelli che possono essere resi disponibili al Fse. Al riguardo, l'Autorità ha ritenuto che la legge di bilancio, nel prevedere che alcuni documenti presenti nel Sistema TS siano resi disponibili al Fse, abbia favorito l'implementazione del Fascicolo con dati e documenti già presenti sull'infrastruttura nazionale di supporto al Fse. Tale intervento normativo non ha però modificato le specifiche disposizioni che disciplinano i singoli flussi di dati e documenti nel Sistema TS. A tali specifiche disposizioni normative occorre quindi far ancora riferimento per individuare le finalità del trattamento e i soggetti destinatari dei suddetti dati e documenti. Il contributo del Garante è inoltre servito ad individuare una soluzione tecnica che consenta, anche nei confronti delle informazioni relative a tale nuovo contenuto informativo del Fse, l'oscuramento di tutti i documenti e i metadati eventualmente collegati al documento su cui l'interessato esercita il diritto di oscuramento.

Nell'ambito dei lavori del tavolo è stato inoltre redatto un modello tipo di informativa utilizzabile dalle regioni per il trattamento dei dati personali effettuato tramite il Fse. Nell'elaborazione di tale modello l'Autorità ha raccomandato di adottare un testo sintetico ed efficace che contenga anche l'indicazione del periodo di conservazione dei dati e dei documenti consultabili tramite il Fse (cfr. art. 13, par. 2, lett. *a*), RGPD).

Oltre alla collaborazione istituzionale in tema di Fse, l'Ufficio è intervenuto anche con riferimento a specifiche fattispecie di violazione della disciplina in materia di protezione dei dati personali nel trattamento effettuato attraverso singoli Fse dei pazienti. In particolare, in un caso oggetto di segnalazione, è stato rilevato che, per un errore di configurazione, un ospedale aveva erroneamente messo a disposizione le schede di dimissione ospedaliera di alcuni pazienti nei Fse di altri soggetti. Sulla vicenda, una volta acquisite rassicurazioni in merito alla modifica della procedura del flusso di integrazione dei Fse in occasione dei ricoveri, è stato avviato un procedimento sanzionatorio (nota 17 gennaio 2018).

Analogamente, l'Ufficio ha accertato che un'azienda sanitaria aveva reso accessibili, tramite il Fse di un paziente, dati e documenti relativi ad un altro soggetto minore di età. L'errore, dipeso dalla mancata applicazione delle regole sull'attività di refertazione ambulatoriale, ha determinato un illecito trattamento dei dati dell'interessato con conseguente avvio di un procedimento sanzionatorio (nota 16 novembre 2017).

Sono state altresì esaminate segnalazioni relative a trattamenti di dati personali effettuati attraverso i *dossier* sanitari di ospedali e aziende sanitarie. Al riguardo sono state richiamate le linee guida in materia di *dossier* sanitario (provv. 4 giugno 2015, n. 164, doc. web n. 4084632) e le misure ivi indicate con riferimento all'individuazione dei soggetti abilitati all'accesso ai *dossier* e ai processi da implementare per delimitare la "profondità" degli accessi agli stessi consentita. Gli interventi dell'Ufficio hanno riguardato non solo casi specifici, ma anche l'applicazione dei principi di protezione dei dati nel processo di unificazione dei sistemi informativi, anche relativi al *dossier* sanitario, a seguito della razionalizzazione dell'assetto delle aziende sanitarie che spesso ha determinato una fusione tra le medesime.

5.1.3. I referti e la documentazione sanitaria

In materia di referti e documentazione sanitaria merita evidenziare, tra gli interventi dell'Autorità, quanto emerso nel corso di un accertamento ispettivo, avviato sulla base di notizie stampa, che ha consentito di accertate alcune anomalie nell'erogazione dei sevizi sanitari *online* offerti da una regione. In particolare, è stato rilevato che, nell'ambito della funzione di invio del promemoria della prenotazione della prestazione sanitaria via *e-mail*, variando il parametro del codice di prenotazione contenuto nel *link* (inviato via *e-mail* all'utente) era possibile visualizzare e/o scaricare i *coupon* di altri assistiti. A seguito dell'intervento dell'Autorità, la regione ha provveduto dapprima a disattivare il servizio e successivamente ad adottare un sistema di codifica della URL del codice di prenotazione che consentisse di superare la predetta criticità. In relazione all'illecito trattamento di dati personali accertato è stato avviato un procedimento sanzionatorio.

In tema di referti, l'Autorità è stata chiamata a pronunciarsi anche in relazione alla consegna a persone diverse da quelle interessate della relazione clinica contenente la descrizione del ciclo di trattamenti effettuati ai fini di procreazione medicalmente assistita. A seguito di una segnalazione, l'Ufficio ha avviato un'istruttoria nei confronti di un centro di procreazione medicalmente assistita, titolare del trattamento, nell'ambito della quale è risultato che la consegna della citata relazione clinica a soggetti diversi dagli interessati era avvenuta per un mero errore materiale

commesso da un incaricato nei cui confronti è stato adottato un richiamo disciplinare. In considerazione tuttavia dell'accertamento di una comunicazione di dati personali di natura sensibile in assenza di un presupposto legittimante è stato avviato un procedimento sanzionatorio (nota 18 settembre 2017).

5.1.4. La tutela della dignità della persona

Attenzione è stata posta alla tutela della dignità delle persone nell'ambito del trattamento di dati personali per finalità di cura. In particolare, l'Ufficio è intervenuto a seguito di una segnalazione relativa alla presenza di studenti tirocinanti durante una visita di controllo effettuata successivamente ad un intervento chirurgico. Al riguardo, all'azienda sanitaria interessata è stato ricordato che l'Autorità ha espressamente previsto che, ove le aziende ospedaliero-universitarie intendano avvalersi di studenti autorizzati, devono indicare nell'informativa da fornire al paziente (art. 13 del Codice) che, in occasione di alcune prestazioni sanitarie, si perseguono anche finalità didattiche, oltre che di cura e prevenzione. Durante tali prestazioni devono essere adottate specifiche cautele volte a limitare l'eventuale disagio dei pazienti, anche in relazione al grado di invasività del trattamento circoscrivendo, ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie (cfr. punto 3.a, provv. 9 novembre 2005, doc. web n. 1191411) (nota 22 novembre 2017).

Analogamente, a seguito di segnalazioni in merito allo svolgimento di colloqui con il personale sanitario presso il letto di degenza alla presenza di altri ricoverati e familiari in visita, l'Ufficio ha rappresentato che, compatibilmente con le esigenze organizzative connesse alla disponibilità dei locali adibiti al ricovero, devono essere adottate misure volte a garantire, quanto più possibile, la riservatezza dei colloqui. È stato inoltre rimarcato che devono essere adottate soluzioni tali da prevenire, durante i colloqui o la raccolta della documentazione di anamnesi, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute nonché cautele volte ad evitare che le prestazioni sanitarie avvengano in situazioni di promiscuità (art. 83, comma 2, lett. *c*) e *d*), punto 3.b), cit. provv. 9 novembre 2005) (nota 26 gennaio 2018).

5.1.5. Il trattamento di dati personali in relazione dell'accertamento dell'infezione da HIV

Nel 2017 l'Ufficio è intervenuto fornendo specifiche indicazioni in merito alle misure a tutela della dignità e della riservatezza dei malati di HIV in occasione dell'erogazione di prestazioni sanitarie; in particolare, sono stati forniti chiarimenti sulle modalità di trasmissione, anche per via telematica, ai donatori di sangue dei referti relativi agli esami ematochimici, con particolare riferimento alla sussistenza di particolari limiti per i risultati relativi all'accertamento dello stato di sieropositività.

L'Ufficio, nel richiamare le disposizioni vigenti in materia di refertazione *online* (linee guida in tema di referti *online*, provv. 19 novembre 2009, doc. web n. 1679033; d.P.C.M. concernente le modalità di consegna, da parte delle aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché di effettuazione del pagamento *online* delle prestazioni erogate dell'8 agosto 2013 su cui il Garante ha espresso il proprio parere 6 dicembre 2012, n. 382, doc. web n. 2223206), ha rappresentato che specifiche previsioni normative prevedono l'obbligo per "gli operatori sanitari che, nell'esercizio della loro professione, vengano a conoscenza di un caso di AIDS, ovvero di un caso di HIV" di "adottare tutte le misure occorrenti per la tutela della riservatezza" e di comunicare i risultati

degli accertamenti diagnostici, diretti o indiretti, "esclusivamente alla persona cui tali esami sono riferiti" (art. 5, commi 1 e 4, l. n. 135/1990). In materia è stato rappresentato inoltre che nel predetto d.P.C.M. è specificato che lo stesso non trova applicazione nei confronti dei referti relativi ad indagini genetiche. Per gli accertamenti sull'HIV, il decreto richiama l'art. 5, l. n. 135/1990, in osservanza di quanto indicato dal Garante nelle predette linee guida in merito alla necessità di tenere conto di quanto previsto da tale disciplina per la comunicazione del risultato diagnostico relativo agli accertamenti dello stato di sieropositività (nota 26 gennaio 2017).

5.2. *I trattamenti di dati relativi alle condizioni di salute per fini amministrativi*

Numerosi sono stati gli interventi dell'Autorità in ordine al trattamento dei dati personali effettuato per finalità amministrative correlate alla cura. In particolare, nei primi mesi del 2017 l'Autorità è venuta a conoscenza da notizie di stampa dell'accordo siglato tra la Presidenza del Consiglio dei ministri e una multinazionale dell'ICT per la realizzazione di un Centro europeo di eccellenza per la salute in Milano e della prevista cessione ad una multinazionale dell'informatica di dati personali relativi a prestazioni sanitarie e farmaceutiche degli assistiti dal Ssn detenuti dalle regioni e dall'Aifa. Al riguardo, sono state richieste informazioni alla Presidenza del Consiglio dei ministri e alla Regione Lombardia (nota 21 febbraio 2017). In considerazione degli elementi forniti dai suddetti Enti, l'Autorità ha evidenziato che l'attuazione dell'accordo può avere un significativo impatto su un numero elevato di interessati, considerato che il trattamento prospettato prevede l'uso di nuove tecnologie nonché l'utilizzo e la comunicazione di dati idonei a rivelare lo stato di salute di una ampia fascia della popolazione. Il Garante ha apprezzato l'invito della Presidenza del Consiglio dei ministri alle parti interessate a informare preventivamente l'Autorità sulle iniziative che saranno promosse al riguardo e ha auspicato che il suddetto coinvolgimento sia realizzato sin dalla fase di elaborazione dei documenti attuativi dell'accordo stesso, al fine di individuare soluzioni condivise rispettose della disciplina in materia di protezione dei dati personali (nota Segretario generale 10 maggio 2017).

Nei mesi successivi il Garante ha continuato a mantenere alta l'attenzione sul trattamento dei dati oggetto del suddetto accordo, rappresentando la necessità di conformare il contenuto dello stesso al nuovo quadro giuridico introdotto dal RGPD, sulla base anche delle specifiche disposizioni di legge che saranno approvate all'esito del processo di adattamento e integrazione del RGPD in forza della delega conferita al Governo dal Parlamento con la legge 25 ottobre 2017, n. 163 (art. 13). Alla luce di ciò, l'Autorità ha evidenziato la necessità che siano meglio definiti aspetti fondamentali in merito al trattamento dei dati personali, quali, tra l'altro, le modalità di comunicazione dei dati, l'attività non compatibile con la qualifica di responsabile del trattamento e la qualifica dei soggetti anche privati coinvolti nel progetto. È stato altresì precisato che spetta al titolare del trattamento, determinare, in modo autonomo, le finalità e i mezzi del trattamento; compete quindi esclusivamente alla regione definire gli ambiti di interesse e individuare le attività di studio tecnologico applicato alla programmazione sanitaria ritenute indispensabili per lo svolgimento delle proprie funzioni istituzionali, anche in relazione all'individuazione dei possibili impieghi dei risultati conseguiti nell'ambito delle predette attività di studio.

Ferma restando la necessità che ogni attività di ricerca risponda ai requisiti etici e metodologici relativi allo specifico settore disciplinare, è stato rappresentato poi

che, nel presupposto del rispetto del principio di liceità del trattamento, il trattamento ipotizzato non può prescindere da una valutazione di impatto sulla protezione dei dati ai sensi dell'art. 35 del RGPD e considerati i criteri individuati dal Gruppo Art. 29.

Considerata la particolare innovatività del progetto, occorrerà anche tener conto delle principali indicazioni formulate a livello internazionale, tra le quali si segnalano le *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data* del Consiglio d'Europa del 23 gennaio 2017, che raccomandano di tenere nella massima considerazione non soltanto le implicazioni giuridiche, ma anche quelle sociali, etiche e tecnologiche nell'uso dei dati (cfr. punto 2) (nota 28 novembre 2017).

Un'ulteriore attività istruttoria svolta dall'Autorità in tale ambito, anche tramite accertamenti ispettivi, ha riguardato i trattamenti dei dati effettuati dalle aziende sanitarie e dall'Aifa, ai fini dell'elaborazione del rapporto OsMed relativo al consumo dei farmaci in Italia. Nell'ambito dell'attività svolta è emersa l'intenzione di modificare le modalità di raccolta dei dati da parte dell'Agenzia ai fini di un più puntuale controllo e monitoraggio delle attività connesse al consumo dei farmaci sul territorio. Sul punto l'Ufficio ha evidenziato che per "dato personale" si deve intendere qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"), direttamente o indirettamente anche mediante un identificativo, come un numero di identificazione (art. 4, n. 1, RGPD). Ciò significa che l'applicazione di tecniche di pseudonimizzazione, pur essendo una misura per la riduzione del rischio di identificazione dell'interessato, non fa venir meno la natura di dato personale e implica, pertanto, la piena applicazione del quadro normativo vigente in materia (cfr. considerando 26, 28, 29 e 78 nonché artt. 4, n. 5, 25 e 32, RGPD). In merito alla realizzazione dei progetti relativi all'analisi dei dati raccolti sul consumo dei farmaci che vedano coinvolti soggetti privati, designati responsabili del trattamento e tenuti ad assolvere precise funzioni, è stato poi evidenziato che, ai sensi del RGPD, qualora un trattamento debba essere effettuato per conto del titolare, quest'ultimo deve ricorrere unicamente a soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del quadro normativo vigente e garantisca la tutela dei diritti dell'interessato (note 1° e 14 dicembre 2017).

L'Autorità ha avuto altresì modo di verificare, sulla base di una segnalazione, la conformità alla disciplina in materia di protezione dei dati personali del trattamento effettuato da una regione attraverso un portale, accedendo al quale era stato possibile visualizzare quietanze di pagamento relative a trattamenti medici effettuati da un'altra persona. È stata quindi avviata un'istruttoria, all'esito della quale è stata riscontrata un'illecita comunicazione a terzi di dati personali, anche sensibili, priva di idonea base normativa e in assenza del consenso dell'interessato, derivante da un malfunzionamento tecnico del sistema che non era previsto nella *check-list* di collaudo e il cui effetto operativo non era immediatamente determinabile fino al suo verificarsi. A fronte di ciò è stata assicurata l'adozione di misure per prevenire il ripetersi in futuro di incidenti analoghi e l'istruttoria si è chiusa con l'avvio di un procedimento sanzionatorio (nota 11 dicembre 2017).

L'Ufficio è altresì intervenuto in merito alla comunicazione ad un familiare del segnalante di informazioni sul suo stato di salute da parte di un'operatrice di un centro diagnostico privato presso il quale questi si era rivolto. A seguito di una richiesta di informazioni, il medesimo centro ha dichiarato che l'operatrice incaricata aveva provveduto a contattare il segnalante, utilizzando i riferimenti dallo stesso rilasciati in occasione della prenotazione (telefono cellulare e, in seconda battuta,

telefono fisso) e rispettando le istruzioni impartite al personale addetto alla gestione delle prenotazioni, che prevedevano di utilizzare esclusivamente i dati conferiti dall'interessato. L'Ufficio, considerata la dinamica dei fatti oggetto di segnalazione, relativa al contenuto di una conversazione telefonica, non disponendo di elementi di valutazione obiettivi, non ha ravvisato elementi sufficienti a qualificare una violazione del Codice né i presupposti per l'adozione di un provvedimento (nota 29 agosto 2017).

In più di un'occasione l'Autorità ha fornito indicazioni in ordine all'applicazione del RGPD. In particolare, in relazione alle modalità di acquisizione del consenso per i dati sanitari nell'ambito di un'applicazione per cellulare, utilizzata da pediatri e genitori di minori per scambiarsi informazioni sulle terapie intraprese, è stato rappresentato che il trattamento ipotizzato, considerata l'estrema delicatezza dei dati trattati, aventi ad oggetto lo stato di salute relativo a minori, nonché l'uso di strumenti elettronici, può rientrare tra quelli che presentano un rischio elevato per i diritti e le libertà delle persone fisiche; pertanto il titolare del trattamento è tenuto ad effettuare una valutazione d'impatto sulla protezione dei dati ai sensi degli artt. 35 e ss. del RGPD (nota 26 settembre 2017).

La medesima valutazione è stata evocata a seguito della trasmissione da parte di una società di un documento recante la predetta valutazione. Al riguardo, è stato evidenziato che il titolare, prima di procedere al trattamento, è tenuto ad effettuare una valutazione dell'impatto sulla protezione dei dati personali dei trattamenti previsti che presentino un rischio elevato per i diritti e le libertà delle persone fisiche, considerati la natura, l'oggetto, il contesto e le finalità del trattamento (artt. 35 e 36). Sul caso specifico, è stato evidenziato che, nella documentazione trasmessa all'Autorità, l'attività della società, avente ad oggetto lo sviluppo di programmi di supporto al paziente e l'erogazione di specifici servizi in favore del medico e dei pazienti che abbiano aderito allo programma in parola, era stata descritta in modo eccessivamente sommario. È stato chiarito che, al di fuori di quanto specificamente previsto dal RGPD nell'ambito della consultazione preventiva e ove ne ricorrano i presupposti (art. 36), non compete all'Autorità esaminare e valutare le modalità e le scelte organizzative poste in essere dal titolare del trattamento. Ove tuttavia il titolare ritenga di avviare una consultazione preventiva ai sensi dell'art. 36 del RGPD, nel trasmettere la documentazione all'Autorità, occorre specificare in modo chiaro quali siano gli ambiti del trattamento che presentano ancora un rischio elevato nonostante le misure specificamente individuate e descritte dal titolare, per i quali è richiesto un parere all'Autorità. Ove, invece, dalla valutazione dell'impatto dei trattamenti sulla protezione dei dati personali, non emergano rischi non adeguatamente attenuati, in conformità al principio di *accountability* la relativa documentazione non deve essere trasmessa all'Autorità, ma conservata a disposizione della stessa in caso di controllo (nota 29 gennaio 2018).

5.2.1. Il trattamento dei dati personali nell'ambito dell'assolvimento degli obblighi vaccinali

Come già evidenziato (v. parr. 2.1.1 e 4.7), il Garante è stato investito da Istituzioni e singoli circa gli aspetti di protezione dei dati personali connessi ai nuovi obblighi vaccinali previsti dall'art. 1, d.l. n. 73/2017 che, al fine di assicurare la tutela della salute pubblica e il mantenimento di adeguate condizioni di sicurezza epidemiologia in termini di profilassi e di copertura vaccinale, prevede che per i minori sino all'età di sedici anni e per tutti i minori stranieri non accompagnati sono obbligatorie e gratuite, in base alle specifiche indicazioni del calendario vaccinale nazionale relativo a ciascuna coorte di nascita.

Il primo intervento dell'Autorità in materia ha riguardato una richiesta formulata da un ufficio scolastico regionale di trasmettere alle aziende sanitarie l'elenco completo dei soggetti iscritti per far fronte, tempestivamente e in modo efficace, alle difficoltà delle aziende sanitarie di gestire le (imminenti) richieste massive di documentazione vaccinale aggiornata da parte dei genitori, e, corrispondentemente, alle esigenze dei genitori ad acquisirla entro i tempi ristretti previsti dal legislatore. Tale trasmissione dei dati avrebbe consentito alle aziende sanitarie interessate di avviare, fin dalla ricezione degli elenchi, la prevista attività di verifica delle singole posizioni e di avvio delle procedure previste (convocazione dei genitori) nonché di pianificare le attività necessarie a mettere a disposizione dei genitori, anche di iniziativa, la documentazione richiesta dal decreto. Il Garante ha accolto tale richiesta consentendo la comunicazione degli elenchi degli iscritti alle scuole perché necessaria allo svolgimento di funzioni istituzionali delle predette amministrazioni che non potrebbero essere altrimenti perseguite, con adeguata tempestività, senza l'utilizzo dei dati oggetto della richiesta (provv. 1° settembre 2017, n. 365, doc. web n. 6765917); in tale occasione è stato evidenziato che le Ausl che lo avessero ritenuto avrebbero potuto inviare la documentazione sull'assolvimento degli obblighi vaccinali direttamente ai genitori, evitando agli stessi l'onere di recarsi presso la struttura sanitaria (limitando, in tal modo, l'afflusso ai casi strettamente indispensabili).

Sollecitato da diverse regioni, è stato altresì rappresentato che la comunicazione da parte delle Ausl alle scuole dell'elenco dei soggetti non in regola con gli obblighi vaccinali doveva essere qualificata come comunicazione di dati a vario titolo sensibili, vuoi in quanto idonei a rivelare lo stato di salute dei minori (tra i soggetti non in regola potrebbero essere ricompresi minori rientranti nei casi di esonero, omissione o differimento connesse a situazioni di morbilità, pregresse o attuali, temporanee o permanenti), vuoi in quanto idonei a rivelare convinzioni filosofiche o di altro genere delle famiglie dei minori interessati (note del Presidente 20 ottobre 2017, doc. web nn. 7037400 e 7055689 e 25 ottobre 2017, doc. web n. 7055771).

Con il decreto legge 16 ottobre 2017, n. 14 (art. 18-*ter*), è stato previsto che, anche per l'anno scolastico 2017/2018, nelle sole regioni e province autonome presso le quali sono già state istituite anagrafi vaccinali, le disposizioni di semplificazione già previste per l'a.s. 2019/2020 relative alla possibilità che le aziende sanitarie locali restituiscano alle scuole gli elenchi dei soggetti che risultano non in regola con gli obblighi vaccinali, siano applicabili a decorrere dall'anno scolastico 2018/2019, nel rispetto delle modalità operative congiuntamente definite dal Ministero della salute e dal Ministero dell'istruzione, dell'università e della ricerca, sentito il Garante. Il predetto decreto prevede poi che, nelle medesime regioni e province autonome, le disposizioni di semplificazione sopra richiamate siano applicabili già per l'anno scolastico in corso, a condizione che il controllo sul rispetto degli adempimenti vaccinali si concluda entro il 1° marzo 2018. In merito a tale disposizione l'Autorità ha manifestato la propria disponibilità ad individuare soluzioni uniformi sul territorio nazionale (nota 23 novembre 2017).

5.3. *I dati genetici*

Anche nel 2017 il Garante ha fornito chiarimenti in ordine al trattamento dei dati genetici. In particolare sono state fornite indicazioni dall'Ufficio con riferimento all'utilizzo di tali dati nell'ambito dell'esecuzione di *test* predittivi. Al riguardo è stato evidenziato che, nell'ambito dell'autorizzazione generale al trattamento dei dati genetici (n. 8/2016), è considerato *test* genetico l'analisi a scopo clinico di uno

5

specifico gene o del suo prodotto o funzione o di altre parti del Dna o di un cromosoma, volta a valutare la maggiore o minore suscettibilità di un individuo a sviluppare malattie multifattoriali (*test* predittivo o di suscettibilità). Ogni trattamento di dati genetici a fini predittivi deve essere pertanto effettuato nel rispetto di quanto previsto nella suddetta autorizzazione. Con specifico riferimento a tali *test*, è stato richiamato quanto previsto dalla Convenzione sui diritti dell'uomo e sulla biomedicina, firmata a Oviedo il 4 aprile 1997, che limita l'espletamento di *test* genetici predittivi ai soli fini medici o di ricerca medica e sulla base di una consulenza genetica appropriata (art. 12 cfr. anche artt. 45 e 46 del codice di deontologia medica del 2014) (nota 30 novembre 2017).

6 La ricerca scientifica e la statistica

6.1. *La ricerca scientifica*

Nel campo della ricerca scientifica merita evidenziare un provvedimento con il quale il Garante ha autorizzato un istituto di ricovero e cura a carattere scientifico e altri centri di cura partecipanti al trattamento dei dati attinenti alla salute dei pazienti affetti da sindrome da sofferenza respiratoria acuta nell'ambito di uno studio multicentrico internazionale di tipo interventistico. L'autorizzazione ammette il trattamento dei dati in assenza di previa informativa e del consenso dei pazienti qualora gli stessi, a seguito delle verifiche dei medici sperimentatori, risultino temporaneamente incapaci di prestarlo e tale incapacità non sia riacquisita prima del termine del previsto periodo di *follow up*. L'autorizzazione è stata limitata ai dati e alle operazioni strettamente indispensabili e pertinenti per la conduzione dello studio. Il Garante ha in particolare tenuto conto dello stato di incoscienza nel quale versavano gran parte dei pazienti eleggibili per lo studio proprio a causa della predetta sindrome da sofferenza respiratoria acuta e ha quindi considerato che le finalità perseguite non potessero essere realizzate mediante il trattamento di dati personali sulla salute riferiti soltanto a persone in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso (provv. 11 maggio 2017, n. 228, doc. web n. 6503911).

In materia si evidenzia che sono in corso anche alcune istruttorie su richieste di autorizzazioni di studi e ricerche con riferimento alle quali non risultano ancora comprovate le circostanze dalle quali derivi l'impossibilità di informare gli interessati ovvero chiarito se gli studi prevedano il coinvolgimento di pazienti minori d'età e, in caso positivo, se sia stata presa in considerazione l'esigenza di adeguare l'esercizio del diritto alla protezione dei dati del minore al suo grado di maturità. In alcuni casi inoltre è stato richiesto di precisare l'ambito di comunicazione dei dati trattati verso destinatari stabiliti in Paesi non appartenenti all'Unione europea e le cautele adottate per l'eventuale trasferimento all'estero nonché il periodo di conservazione dei dati in una forma che consenta, anche indirettamente, l'identificazione dei pazienti interessati una volta concluso lo studio (note 9 maggio, 13 ottobre, 30 novembre e 1° dicembre 2017).

Novella al Codice

In materia di ricerca scientifica merita evidenziare una novella legislativa intervenuta nel 2017 che prevede una nuova fattispecie di trattamento (art. 28, comma 1, lett. *b*), l. 20 novembre 2017, n. 167). Secondo quanto indicato dall'art. 110-*bis* del Codice, nell'ambito delle finalità di ricerca scientifica o per scopi statistici, il Garante può autorizzare il riutilizzo dei dati, anche sensibili, a condizione che siano adottate idonee forme preventive di minimizzazione e di anonimizzazione dei dati a tutela degli interessati; tale previsione esclude il trattamento di dati genetici per tali finalità (in merito v. l'intervista del presidente Soro "Riutilizzo dati sanitari a fini ricerca scientifica e RGPD", TG 2 - "Lavori in corso": doc. web n. 7296327). L'autorizzazione del Garante è adottata entro quarantacinque giorni dalla richiesta, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di

autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del riutilizzo dei dati, anche sotto il profilo della loro sicurezza.

Malattie rare

In relazione alla richiesta di autorizzazione alla trasmissione di dati da parte delle regioni al registro nazionale malattie rare, l'Ufficio ha fornito riscontro all'Istituto superiore della sanità richiamando, in primo luogo, la specifica (ed articolata) disciplina di settore in materia di sorveglianza delle malattie rare, consistente, in particolare, nel d.m. 18 maggio 2001, n. 179, sul quale il Garante ha espresso il proprio parere in data 27 ottobre 1999 (doc. web n. 41167); nel d.P.C.M. 3 marzo 2017, che inserisce il registro nazionale e registri regionali delle malattie rare tra i sistemi di sorveglianza di rilevanza nazionale e regionale, già disciplinati dalla normativa vigente a livello nazionale (All. B); nella scheda n. 12, relativa all'attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, dell'All. A allo schema tipo di regolamento per i trattamenti dei dati sensibili e giudiziari di competenza delle regioni e delle province autonome, delle aziende sanitarie, degli enti e agenzie regionali/provinciali, nonché degli enti vigilati dalle regioni e dalle province autonome (su cui il Garante ha espresso parere favorevole: provv. 13 aprile 2006, doc. web n. 1272225 e provv. 26 luglio 2012, doc. web n. 1915390); nell'accordo, ai sensi dell'art. 4, d.lgs. 28 agosto 1997, n. 281, tra il Governo, le Regioni e le Province autonome di Trento e Bolzano sul riconoscimento di Centri di coordinamento regionali e/o interregionali, di presidi assistenziali sovraregionali per patologie a bassa prevalenza e sull'attivazione dei registri regionali ed interregionali delle malattie rare (Accordo Conferenza Stato-Regioni del 10 maggio 2007, CSR Rep. Atti n. 103/CSR).

È stato quindi evidenziato che la comunicazione dei dati sanitari al registro nazionale delle malattie rare non necessita di una specifica autorizzazione del Garante, tenuto conto che, già alla luce del quadro normativo di settore, può rinvenirsi la necessità che le regioni alimentino il registro nazionale delle malattie rare, garantendo la trasmissione dei dati all'Istituto superiore di sanità presso il quale il predetto registro è istituito (nota 6 ottobre 2017).

Registro tumori Regione Lazio

Il Garante ha reso parere favorevole su una versione aggiornata dello schema di regolamento di attuazione e integrazione della legge regionale 12 giugno 2015, n. 7, istitutiva del Registro tumori di popolazione della Regione Lazio che, in larga misura, ha tenuto conto delle osservazioni formulate dall'Ufficio. Il Registro, che costituisce parte integrante del Sistema informativo sanitario regionale, ha lo scopo di raccogliere dati statistici sull'incidenza, la prevalenza e la sopravvivenza dei casi di tumore, anche infantili, all'interno della Regione, nonché di potenziare la prevenzione e la valutazione delle terapie, e di supportare gli studi epidemiologici e i programmi di ricerca oncologica. Il regolamento disciplina l'assetto organizzativo e le modalità di funzionamento del Registro e le garanzie sulla riservatezza e individua i tipi di dati sensibili trattati, le operazioni eseguibili, le fonti dei flussi informativi, l'ambito della comunicazione delle informazioni.

Titolare del trattamento è il Dipartimento di epidemiologia del servizio sanitario regionale presso cui il Registro è allocato e che ne cura la gestione amministrativa, tecnica ed informatica. Per assicurare elevati standard di riservatezza, lo schema di regolamento prevede specifiche disposizioni sull'obbligo di rendere una dettagliata informativa ai malati e una serie di misure a tutela dei dati personali, quali l'utilizzo di codici identificativi, la conservazione separata dei dati anagrafici da quelli sanitari, l'accesso selettivo ai dati da parte dei soggetti autorizzati, sistemi antivirus costantemente aggiornati e sistemi anti-malware.

Con riguardo al flusso di dati sui tumori infantili proveniente dall'Associazione italiana di ematologia e oncologia pediatrica (Aieop), il Garante ha chiesto alla Regione di verificare, in particolare, la legittimità del trattamento dei dati personali contenuti in tale archivio, riservandosi di svolgere i necessari controlli per verificarne la conformità alla normativa di protezione dei dati.

L'Autorità ha chiesto inoltre di integrare il disciplinare con idonee misure di sicurezza fisica anche per l'accesso ai locali del Registro secondo una documentata procedura (provv. 20 marzo 2017, n. 165, doc. web n. 6275462).

6.2. *La statistica e il censimento permanente*

Programma statistico nazionale

Nel 2017 il Garante si è espresso sull'aggiornamento 2018-2019 del Programma statistico nazionale 2017-2019, ai sensi del codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica trattati nell'ambito del Sistema statistico nazionale (Sistan), All. A3 al Codice, relativo a circa 350 lavori statistici svolti dall'Istat e da 57 soggetti Sistan (parere 2 marzo 2017, n. 87, doc. web n. 6239992).

Numerose indicazioni sono state fornite all'Istat, già nel corso dell'istruttoria, riguardo all'esatta individuazione dei tipi di dati personali trattati (con riferimento alle tipologie di dati sensibili oggetto di rilevazione e alla definizione di dato giudiziario), alla corretta indicazione della denominazione delle banche dati utilizzate nei lavori statistici che impiegano fonti amministrative, all'indicazione delle fonti normative che impongono l'obbligo di risposta anche in relazione ai dati sensibili, alla descrizione delle variabili riferibili ai dati personali oggetto di rilevazione, alla precisazione dei motivi per i quali sono conservati i dati identificativi diretti e delle ragioni per le quali è impossibile conservarli separatamente dagli altri dati personali, nonché alla limitazione dell'ambito di comunicazione dei dati e alla diffusione di variabili in forma disaggregata.

Nel parere, il Garante ha, in primo luogo, richiamato l'attenzione sul tema dell'accesso ai microdati per finalità di ricerca in base al nuovo quadro regolatorio introdotto dall'art. 5-*ter*, d.lgs. 14 marzo 2013, n. 33, disposizione che stabilisce i requisiti per l'ente di ricerca che intende accedere ai dati, le modalità di rilascio dei dati nonché le operazioni di trattamento eseguibili, facendo divieto di effettuare trattamenti diversi da quelli previsti nel progetto di ricerca, conservare i dati elementari oltre i termini di durata del progetto, comunicare i dati a terzi e diffonderli. In secondo luogo, il Garante, pur valutando positivamente il fatto che, in alcune rilevazioni che comportano il trattamento di dati personali di carattere particolarmente delicato, il titolare del lavoro statistico abbia previsto di cancellare, o evitare di raccogliere, i dati che consentono l'identificazione diretta degli interessati, ha evidenziato che tale garanzia potrebbe essere compromessa nel caso in cui i dati, privati degli identificativi diretti, vengano, in seguito, utilizzati in altri lavori statistici in cui sono presenti numerose ulteriori fonti amministrative con elevati rischi di reidentificazione degli interessati. Occorre quindi che il titolare del lavoro statistico effettui, con particolare attenzione, la scelta delle variabili da utilizzare in caso di ulteriori lavori statistici, per evitare che possano venir meno le garanzie introdotte per gli interessati con l'eliminazione dei dati identificativi diretti.

È stata inoltre avviata la verifica preliminare sui lavori IST-02270 Sistema di integrazione logico-fisica di microdati amministrativi e statistici (Sim) e IST-02264 Base integrata di microdati statistici per l'analisi dell'occupazione, che potranno essere avviati solo una volta individuate le necessarie garanzie relative alla qualità e

alla sicurezza dei dati, alle modalità del trattamento e agli effetti che può determinare sugli interessati, soprattutto in considerazione dell'accresciuto numero di banche dati amministrative di cui si è prospettato l'utilizzo (in totale, circa 20 per la Base integrata e circa 70 per il Sim, tra le quali rileva, in particolare, l'introduzione del Sistema informativo integrato dell'Acquirente unico dell'energia, con il codice fiscale del cliente, la localizzazione e il consumo energetico).

Sono state formulate inoltre alcune osservazioni su specifici lavori statistici, ponendo l'attenzione sul contenuto dei questionari, sull'opportunità della conservazione dei dati identificativi diretti, sull'eventuale trattamento di dati genetici e sui termini per la conservazione dei dati personali, specie di minori.

Ulteriori rilievi sono stati formulati sul prospetto IST-02589 "Uso a fini statistici dei *big data*" che coinvolgono l'utilizzo di dati personali, ribadendo che questi dati rappresentano un ampio patrimonio informativo il cui l'utilizzo comporta specifici rischi per la riservatezza e la protezione dei dati personali degli interessati, tenuto anche conto che, grazie alle nuove tecnologie e alle nuove tecniche di analisi, elaborazione e interconnessione dei dati, risulta spesso possibile la reidentificazione di un interessato anche attraverso informazioni apparentemente anonime (cd. *single-out*). Pertanto, nella misura in cui venga assicurata la non identificabilità dell'interessato, ovvero i dati utilizzati non siano riconducibili alla definizione di dato personale, i *big data* possono essere utilizzati liberamente, anche a fini statistici, mentre, laddove l'utilizzo comporti il trattamento di dati personali, ovvero emerga la possibilità di una reidentificazione dell'interessato, trova piena applicazione la normativa in materia di protezione dei dati personali anche in caso di scopi statistici.

Censimento permanente

Come anticipato (v. par. 2.1.1), il Garante ha esercitato il proprio potere di segnalazione al Parlamento e al Governo in relazione all'art. 29, d.d.l. di bilancio per il 2018, foriero di "gravi preoccupazioni per i profili attenenti al rispetto dei diritti fondamentali degli interessati, specie in relazione alla disciplina sulla protezione dei dati personali". In particolare, tale disposizione ha previsto l'integrazione, a fini statistici, presso l'Istat, di archivi amministrativi riferiti alla totalità della popolazione e l'utilizzo massivo dei dati ivi contenuti inerenti ad ogni aspetto dello sviluppo della vita privata e relativi anche ai minori (informazioni demografiche, sociali, fiscali, lavorative, scolastiche, universitarie, oltre che dati sull'appartenenza a famiglie, sulla presenza sul territorio e gli spostamenti, nonché sui consumi energetici individuali); con una successiva ricaduta amministrativa sulla revisione delle anagrafi della popolazione residente fondata sull'elaborazione automatizzata dei dati, contenuti nei predetti archivi, attraverso tecniche di *linkage* e di georeferenziazione (nota del Presidente 7 novembre 2017, doc. web n. 7447536).

Il nuovo censimento permanente – peraltro confermato nella stesura definitiva della legge di bilancio (art. 1, commi 227-237, l. n. 205/2017) – attraverso l'utilizzo di dati amministrativi che consentono la diretta identificazione degli interessati mediante tecniche di profilazione, nonostante la segnalazione dell'Autorità, si propone quindi di classificare ciascun individuo in relazione alla probabilità sua e della sua famiglia "di presenza/assenza in un dato ambito territoriale", anche al fine di comunicare alle competenti amministrazioni comunali i dati individuali dei soggetti trattati per la successiva revisione delle anagrafi.

Al riguardo, l'Autorità ha, in primo luogo, osservato che, innovando profondamente la disciplina delle modalità di realizzazione dei censimenti permanenti, tali disposizioni intervengono su materie estranee di regola alla legge di bilancio, con rilevanti ripercussioni sul diritto alla riservatezza e alla protezione dei dati personali degli interessati, che richiederebbero invece un vaglio parlamentare secondo le procedure ordinarie e non quelle tipiche dei documenti di bilancio.

Nel 2015 il Garante aveva già avuto modo di rappresentare all'Istat e alla Presidenza del Consiglio dei ministri le gravi criticità relative alle ricadute amministrative del censimento (cfr. pareri 29 ottobre 2015, n. 566, doc. web n. 4476104 e 15 ottobre 2015, n. 536, doc. web n. 4481301). In particolare, era già stato evidenziato che i dati trattati per scopi statistici non possono essere utilizzati per altre finalità, né comportare ricadute personalizzate sugli interessati, in ossequio alla normativa sulla protezione dei dati personali (art. 105 del Codice) e ai principi internazionali ed europei al riguardo.

Nella segnalazione, l'Autorità ha ribadito che, in base ai principi di matrice internazionale ed europea, ai quali il Codice dà attuazione, "dovrebbe essere severamente proibito" l'uso di dati raccolti a fini statistici per altri scopi, ad esempio, amministrativi, giuridici o fiscali, oppure per condurre verifiche nei confronti delle unità statistiche (cfr. considerando n. 27, regolamento 2009/223/CE sulle statistiche europee e, a livello internazionale, l'art. 4, raccomandazione del Consiglio d'Europa N. R (97)18 relativa alla protezione dei personali raccolti e trattati per scopi statistici).

È stato poi evidenziato che tali garanzie sono ribadite anche nel RGPD, ai sensi del quale "La finalità statistica implica che il risultato del trattamento per finalità statistiche non siano dati personali, ma dati aggregati, e che tale risultato o i dati personali non siano utilizzati a sostegno di misure o decisioni riguardanti persone fisiche specifiche" (cfr. considerando 162).

È stato inoltre precisato che le precedenti modalità di revisione post-censuaria delle anagrafi, previste nel regolamento anagrafico (d.P.R. n. 223/1989) – in base alle quali veniva disposta la cancellazione dall'anagrafe per irreperibilità in occasione di censimento – risultavano compatibili con l'ordinamento vigente in materia di protezione dei dati personali, in quanto l'interessato era direttamente coinvolto nella raccolta dei dati (che avveniva presso il medesimo), come correttamente specificato nelle informative predisposte dall'Istat, già in origine per le due diverse finalità (amministrativa e statistica).

Ulteriori particolari criticità sono state segnalate per il prospettato utilizzo, nell'ambito del censimento permanente, dei dati contenuti nel Sistema informativo integrato dell'Acquirente unico, dal momento che la sua costituzione non è stata sottoposta al parere dell'Autorità, contrariamente a quanto prevede la legge istitutiva (cfr. art. 1-*bis*, l. n. 129/2010). Poiché questo sistema informativo contiene una mole di dati assai significativa, comprendente tra gli altri dati sui consumi individuali per fascia oraria di energia e gas e, quindi, anche informazioni idonee a rivelare lo stato di salute delle persone interessate (come quelle riferite a macchinari salvavita), il Garante si è riservato di effettuare una specifica valutazione.

7 I trattamenti in ambito giudiziario e da parte delle Forze di polizia

7.1. *I trattamenti in ambito giudiziario*

Sicurezza nelle intercettazioni

Con provvedimento 26 gennaio 2017, n. 26 (doc. web n. 6003325) il Garante è nuovamente intervenuto sulla delicata materia delle misure di sicurezza nelle attività di intercettazione da parte delle Procure della Repubblica, già oggetto delle prescrizioni contenute nel provvedimento 18 luglio 2013, n. 356 (doc. web n. 2551507) ed i cui termini per l'adempimento, sulla base della documentazione trasmessa dal Ministero dell'interno, erano stati inizialmente differiti al 31 gennaio 2017 (cfr. provv. 28 luglio 2016, n. 336, doc. web n. 5385167); sulla base degli approfondimenti svolti nell'ambito di un tavolo di lavoro a carattere inter-istituzionale e dell'esperienza maturata in sede di attuazione delle prescrizioni impartite dall'Autorità, il termine per l'adempimento è stato così ulteriormente differito al 31 dicembre 2017.

Pubblicazione di sentenze a fini di informazione giuridica

Anche nel 2017 l'Autorità si è occupata del delicato tema della pubblicazione *online* delle sentenze contenenti dati personali sensibili o comunque relativi a minori per finalità di informazione giuridica. In particolare è stata lamentata la pubblicazione sul sito di una nota testata giornalistica del testo integrale di una sentenza delle Sezioni Unite della Corte di cassazione, relativa ad una vicenda che ha coinvolto la reclamante ed i propri figli minori, i quali, per effetto dei fatti narrati nella sentenza, avrebbero subito pregiudizio nelle loro relazioni, in particolare nell'ambiente scolastico. Ciò nonostante il divieto di diffusione delle generalità e di altri dati identificativi delle parti in causa annotato a margine della sentenza ai sensi dell'art. 52, comma 2, del Codice. A seguito dell'intervento dell'Autorità, poiché la testata giornalistica aveva provveduto sia alla cancellazione che alla deindicizzazione della sentenza dal sito internet della società, il reclamo è stato archiviato avendo la condotta esaurito i suoi effetti (nota 7 marzo 2017).

Pubblicazione di sentenze di condanna nell'albo pretorio *online*

Un comune ha posto un quesito in merito alla pubblicazione di sentenze penali di condanna e di altre pene accessorie nell'albo pretorio *online*, chiedendo in particolare se gli atti e la documentazione trasmessi da parte delle Procure della Repubblica necessitano di pubblicazione integrale o di parziale oscuramento dei dati. Al riguardo, ferma restando la competenza esclusiva dell'autorità giudiziaria in merito alle modalità di esecuzione dei propri provvedimenti, è stato rilevato che ai sensi dell'art. 36 c.p. la pubblicazione della sentenza di condanna quale pena accessoria "è fatta per estratto, salvo che il giudice disponga la pubblicazione per intero; essa è eseguita d'ufficio e a spese del condannato". Pertanto, ove il giudice non disponga espressamente la pubblicazione della sentenza in forma integrale, questa deve essere compiuta per estratto. Ulteriormente, è stato ricordato che l'art. 36 del regolamento per l'esecuzione del codice di procedura penale (d.m. 30 settembre 1989, n. 334) prescrive che l'estratto del provvedimento giudiziale contiene le generalità della persona nei confronti della quale deve essere eseguito, l'imputazione, il dispositivo e, quando ne è il caso, l'attestazione che non è stata proposta impugnazione od opposizione (nota 20 luglio 2017).

Produzione di atti e documenti in giudizio

Con riferimento alla produzione documentale in sede giudiziaria, il Garante, rispondendo a segnalazioni degli interessati, nel ricordare preliminarmente che l'art. 24, comma 1, lett. *f*), del Codice consente il trattamento di dati personali senza

consenso laddove lo stesso sia necessario 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 stabilisce 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.

In particolare, un segnalante ha lamentato che l'istituto di credito presso il quale prestava servizio, nel giudizio avente ad oggetto il rapporto di lavoro, avrebbe prodotto documenti relativi agli intercorsi rapporti finanziari, irrilevanti nel rapporto dedotto in giudizio. In sostanza, la società, con la quale il segnalante all'epoca dei fatti intratteneva anche rapporti di natura bancaria, violando gli obblighi di lealtà e riservatezza cui era tenuta nella qualità di esercente attività bancaria, avrebbe prodotto in giudizio i predetti documenti inerenti ai rapporti bancari, privi di alcuna rilevanza nel contenzioso nel quale erano stati prodotti. L'Autorità, richiamando l'art. 160, comma 6, del Codice, ha archiviato la segnalazione, poiché la competenza è del giudice ordinario (nota 20 luglio 2017).

In altra vicenda, il segnalante ha lamentato che, nel corso di un giudizio, le controparti avrebbero prodotto, a fini probatori, la registrazione, effettuata ad insaputa dell'interessato e senza il suo consenso, di una conversazione intercorsa presso il proprio studio legale con le suddette controparti. La registrazione sarebbe stata effettuata da una terza persona estranea alla lite e successivamente indicata come teste nel procedimento. L'Autorità ha richiamato l'art. 160, comma 6, del Codice, e inoltre ricordato che il trattamento dei dati personali effettuato per far valere o difendere un diritto non richiede né l'informativa all'interessato (art. 13, comma 5, lett. *b*), né il suo consenso (art. 24, comma 1, lett. *f*); ciò sia in corso di causa che nella fase propedeutica all'instaurazione di un eventuale giudizio, anche al fine di verificare con le parti se vi sia un diritto da tutelare utilmente in sede giudiziaria (cfr. provv. 6 novembre 2008, n. 60, doc. web n. 1565171); la segnalazione è stata pertanto archiviata (nota 20 luglio 2017).

In un altro caso i reclamanti hanno lamentato che, nell'ambito di procedimento instaurato ex art. 700 c.p.c. per asseriti atti di concorrenza sleale da parte di una società di cui i reclamanti erano amministratori e soci, il consulente tecnico d'ufficio (Ctu) delegato avrebbe effettuato un trattamento illecito di dati personali. Nell'eseguire la descrizione del contenuto dei sistemi informatici reperiti nella sede sociale, questi avrebbe estratto i dati da esaminare attraverso copie forensi contenenti anche dati personali dei soci, estranei al giudizio nel quale sono stati acquisiti. In tale circostanza, l'Autorità ha ritenuto che l'acquisizione degli elementi e la valutazione della pertinenza dei dati acquisiti dagli ausiliari del giudice compete in via esclusiva all'autorità giudiziaria la cui decisione viene assunta nel giudizio in contraddittorio con le parti, essendo necessario per l'attuazione della misura cautelare che tutti i dati presenti nei sistemi informatici fossero conosciuti dal giudice, dalle parti, dai loro difensori e consulenti tecnici (nota 22 dicembre 2017).

In un reclamo il debitore lamentava la notifica di un atto di pignoramento presso terzi a ben 26 enti, indicati come terzi pignorati, sicché l'invio massivo dell'atto di pignoramento ha fatto sì che informazioni lesive dell'onore della persona interessata giungessero immotivatamente a soggetti terzi, con assoluto squilibrio tra l'esiguità dell'importo pignorato e l'abnorme numero di soggetti destinatari dell'atto esecutivo. Al riguardo si è rilevato che l'atto contestato si inseriva nel processo di esecuzio-

Notificazioni di atti giudiziari

ne, volto ad ottenere la soddisfazione effettiva di un diritto accertato nella fase di cognizione, e che spetta al giudice, ove ritualmente richiesto, la competenza a valutare la liceità del trattamento dei dati personali dell'interessato. Si è pertanto esclusa la competenza dell'Autorità (nota 9 marzo 2017).

Con riferimento ad altre segnalazioni con cui si lamentava la notifica di atti giudiziari contenuti in buste con l'indicazione di dati ritenuti eccedenti e non pertinenti, il Garante ha rappresentato che, trattandosi di atti inerenti al giudizio, la loro valutazione spetta al giudice adito ai sensi dell'art. 160, comma 6, del Codice.

In un caso, in particolare, la segnalante ha lamentato di aver ricevuto, presso il proprio indirizzo di residenza, la notifica di un atto giudiziario contenuto in una busta recante oltre al nome, cognome e indirizzo, anche la data di nascita e il codice fiscale.

L'Autorità ha ritenuto, infatti, che nel caso di specie rileva un trattamento effettuato per finalità di giustizia (cfr. art. 47 del Codice), trattandosi di atto necessario a dare impulso al processo di esecuzione, disciplinato dal codice di rito quanto a validità ed efficacia, e sottoposto alle valutazioni del giudice. È stato osservato che, in applicazione del citato art. 160, comma 6, la fattispecie è regolata dalla disciplina delle notificazioni a mezzo posta di atti giudiziari e, segnatamente, che l'art. 3, comma 2, l. n. 890/1982 (che indica gli elementi da riportare sulla busta contenente l'atto giudiziario) disciplina elementi che il giudice potrebbe essere chiamato a valutare per decidere della validità ed efficacia della notifica (note 24 ottobre 2017 e 18 gennaio 2018). Pertanto è stato ritenuto che pronunciarsi su tali profili, che potrebbero essere oggetto del giudizio sulla validità della notificazione, non rientri nella competenza dell'Autorità.

Richiesta del domicilio del condannato per far valere pretese risarcitorie

L'ufficio amministrativo di un tribunale ha chiesto conferma al Garante della ritenuta non ostensibilità del domicilio attuale di persona condannata, richiesto dall'avvocato di parte civile per fare valere nei confronti del condannato stesso pretese risarcitorie. Il Garante ha ritenuto corretta l'opinione dell'ufficio in quanto, ai sensi dell'art. 18 del Codice, la comunicazione a privati da parte di un soggetto pubblico può avvenire solo se prevista da norma di legge o regolamento (nota 9 marzo 2017).

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

A seguito di segnalazioni ricevute, anche nel 2017 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 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.

7.3. *L'individuazione dei trattamenti non occasionali effettuati con strumenti elettronici per finalità di polizia e le modalità di attuazione dei principi del Codice rispetto al trattamento dei dati effettuato per le finalità di polizia*

A seguito di un'intensa attività di collaborazione istituzionale con il Ministero dell'interno per comprendere appieno le specificità dei diversi trattamenti ed assicurare il rispetto delle regole in materia di protezione dati, nella prospettiva di un corretto bilanciamento tra le esigenze delle forze di Polizia ed i diritti delle persone, in particolare nei riguardi di trattamenti massivi di dati di persone non oggetto di specifica attenzione da parte delle forze dell'ordine, sono stati resi il parere sugli schemi

di d.P.R., ai sensi dell'art. 57 del Codice, sull'attuazione dei principi di protezione dei dati personali per i trattamenti svolti per finalità di polizia dagli organi preposti ed il parere sullo schema di decreto del Ministero dell'interno, che individua i trattamenti effettuati dal Ced del Dipartimento della pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi, ovvero da organi di pubblica sicurezza o altri soggetti pubblici, di cui all'art. 53, comma 3, del Codice (cfr. par. 3.3.1).

I pareri riguardano, in particolare, uno schema di decreto ministeriale recante l'individuazione dei trattamenti non occasionali effettuati per finalità di polizia eseguiti con strumenti elettronici, previsto dall'art. 53 del Codice (provv. 23 febbraio 2017, n. 74, doc. web n. 6197012), e due schemi di decreto del Presidente della Repubblica che, secondo quanto previsto dall'art. 57 del Codice, disciplinano le modalità di attuazione dei principi del Codice al trattamento dei dati effettuato per le finalità di polizia: il primo, a contenuto generale, è riferito a tutti i trattamenti non occasionali di dati personali effettuati, con strumenti elettronici, da Forze di polizia (provv. 2 marzo 2017, n. 86, doc. web n. 6197365); il secondo riguarda specificamente i trattamenti effettuati dal Centro elaborazioni dati della Polizia di Stato (provv. 26 luglio 2017, n. 337, doc. web n. 6826534).

Lo schema di d.m., oggetto di una complessa istruttoria condotta dagli uffici del Garante in stretta collaborazione con il Ministero, individua nel dettaglio i trattamenti permanenti effettuati dalle Forze di polizia, compresa la gestione delle maggiori banche dati (Ced, Afis, Dna), le relative fonti normative ed il titolare del trattamento stesso. Ciò consente alla collettività, tra l'altro, di conoscere quante e quali sono le banche dati gestite dalle Forze di polizia e quali sono le operazioni che possono essere effettuate sui loro dati personali. Potranno così essere immediatamente identificati i soggetti cui eventualmente rivolgersi per avere informazioni e poter esercitare i propri diritti (anzitutto il diritto di accesso nelle forme previste dalla legge). Nel rendere il parere il Garante ha chiesto, tra l'altro, di escludere dalla tipologia di trattamenti finalizzati all'attività di polizia quelli svolti per finalità amministrative, eliminando i trattamenti per i quali non risulti dimostrata una correlazione diretta con la finalità di polizia (rilascio di licenze, autorizzazioni, nulla osta da parte del Ministero, Prefetture, Questure). Il d.m. è stato adottato dal Ministro dell'interno il 24 maggio 2017 (e pubblicato sulla G.U. n. 145 del 24 giugno 2017, S.O).

Anche gli schemi di d.P.R. di attuazione dell'art. 57 del Codice sono stati oggetto di una intensa attività preparatoria condotta dal Ministero dell'interno con gli uffici del Garante, e le versioni finali recepiscono molte delle richieste avanzate dall'Autorità in fase istruttoria. Circa lo schema di d.P.R. a contenuto generale (nella sua veste definitiva adottato come d.P.R. 15 gennaio 2018, n. 15 in G.U. 14 marzo 2018, n. 61), il Garante ha chiesto, in particolare, di integrare il testo, sottoponendo alle regole in materia di protezione dei dati tutti i tipi di trattamenti che presentano rischi specifici per la persona (banche di dati genetici, biometrici, dati relativi all'ubicazione, banche dati basate su particolari tecniche di elaborazione delle informazioni, ecc.) e di stabilire tempi di conservazione dei dati commisurati alle finalità della raccolta, più brevi di quelli originariamente previsti, ritenuti immotivatamente lunghi. In particolare, non devono essere conservati per più di 90 giorni i dati di persone nei confronti delle quali non è emerso alcun rilievo (ad es., individui identificati a seguito di controlli occasionali del territorio). Sono state chieste, inoltre, regole specifiche per la raccolta e l'uso di immagini acquisite con i droni, in quanto la particolare tecnologia utilizzata può comportare elevati rischi per le persone. Il d.P.R. non si applica ai dati personali trattati per finalità amministrative, che devono anche essere conservati separatamente da quelli registrati per finalità di polizia e che sono soggetti alle regole generali del Codice.

Per quanto riguarda lo schema di d.P.R. relativo ai trattamenti effettuati dal Centro elaborazioni dati della Polizia di Stato (non ancora adottato), il Garante ha ribadito che le disposizioni ivi contenute sono solo necessarie ad esplicitare i principi e le modalità fissati nel d.P.R. generale ai trattamenti effettuati dal Ced, alle cui disposizioni viene di volta in volta operato il rinvio, e non a porsi come nuovo e diverso provvedimento attuativo dell'art. 57, seppur limitatamente ai trattamenti operati dal Ced.

Inoltre, considerata la complessità e l'importanza del Ced, è stata sottolineata la necessità di prevedere misure di sicurezza adeguate ai rischi del trattamento, anche alla luce delle prescrizioni in materia impartite negli anni dal Garante.

7.4. *La banca dati del Dna*

Con provvedimento del 9 marzo 2017, n. 127 (doc. web n. 6163803) è stato reso un parere favorevole, seppur condizionato nei termini di seguito sintetizzati, sulla bozza dell'ultimo dei decreti attuativi che regolamentano la banca nazionale del Dna, grazie al quale viene data piena attuazione alla disciplina necessaria per lo scambio dei dati sul Dna per le finalità di cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità internazionale.

Il testo, predisposto dal Ministero dell'interno di concerto con il Ministro della giustizia, definisce le modalità di cancellazione dei profili genetici, di distruzione dei campioni biologici, di immissione e aggiornamento e conservazione dei dati delle persone censite, come i condannati in via definitiva o chi è stato sottoposto a misure cautelari per reati dolosi gravi.

Il Garante ha evidenziato la necessità di maggiori garanzie sull'aggiornamento dei dati, sulla cancellazione di quelli riferibili a persone assolte con sentenza definitiva e regole chiare per l'accesso alle informazioni da parte delle Istituzioni nazionali. In particolare, è stato richiesto che le informazioni genetiche e gli altri dati personali contenuti nella banca dati siano aggiornati costantemente, anche alla luce delle comunicazioni processuali, e non in base a intervalli predeterminati, così da assicurarne l'esattezza. A tal proposito è stata segnalata la necessità di cancellare prontamente tutti i dati riferibili a chi è stato assolto con sentenza definitiva perché il fatto non sussiste, perché l'imputato non lo ha commesso, perché il fatto non costituisce reato o perché il fatto non è previsto dalla legge come reato.

Nel provvedimento è stata sottolineata l'importanza di fornire un'adeguata informativa alle persone i cui profili sono registrati in banca dati ed evidenziata la necessità di chiarire le regole che impongono la cancellazione di un profilo di Dna, di specificare dove saranno memorizzate le informazioni e di individuare con maggiore precisione quali siano i soggetti nazionali che hanno il diritto di accedere a dati così delicati.

7.5. *Altri interventi riguardanti i trattamenti di dati da parte delle Forze di polizia*

L'Autorità ha reso un parere all'Anac in merito ad un protocollo d'intesa con la Guardia di finanza relativo ai rapporti di collaborazione tra le due Istituzioni e concernente, tra l'altro, uno scambio di dati di tipo bidirezionale. In particolare il menzionato protocollo avrebbe consentito all'Anac di porre a disposizione della Guardia di finanza determinate informazioni della banca dati nazionale dei contratti pubblici e alla Guardia di finanza di utilizzare le stesse per alimentare il proprio sistema informativo (Mo.Co.P.), il quale consente, tra l'altro, di incrociare i dati provenienti

da Anac con ulteriori informazioni della banca dati della Guardia di finanza. Ciò al fine di produrre indici di rischio riferiti ad ogni singolo appalto e di renderli disponibili all'Anac per le proprie attività istituzionali di controllo e verifica. Tali indici di rischio non sono connessi a dati di polizia presenti all'interno del patrimonio informativo del Corpo, ma derivano unicamente dai dati forniti dall'Anac e/o da dati di contesto estratti da altre fonti (in particolare Anagrafe tributaria e Infocamere). Il Garante, a seguito di un approfondito esame delle norme di legge e di regolamento che disciplinano le attività istituzionali di entrambi gli enti ed i rapporti di reciproca collaborazione, ha espresso parere favorevole sul protocollo d'intesa, condizionato al recepimento di alcune modifiche tecniche (provv. 15 giugno 2017, n. 284, doc. web n. 6634563).

Soggetti alloggiati nelle strutture ricettive locali

L'Autorità ha inoltre reso un parere al Ministero dell'interno relativo alla fondatezza della richiesta, formulata da una Direzione provinciale dell'Agenzia delle entrate ad una questura, diretta ad ottenere i dati, detenuti dalle questure sulla base dell'art. 109 del Tulps, relativi ai soggetti alloggiati nelle strutture ricettive locali per "una proficua azione di prevenzione e contrasto all'evasione" (richiamando l'art. 32, comma 1, n. 5, d.P.R. n. 601/1973 e l'art. 51, comma 2, n. 5, d.P.R. n. 633/1972). Il Garante ha ritenuto che tale ostensione sia contraria alle disposizioni in materia di tutela dei dati personali, in quanto il trattamento dei dati degli "alloggiati" da parte delle questure è ammesso solo in quanto svolto dalle Forze di polizia, sulla base di specifica base normativa, ossia "correlato all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria svolti ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati" (art. 53, comma 1, del Codice). Le Forze di polizia possono effettuare sui dati personali detenuti solo attività consentanee a tali finalità e, comunque, previste da specifiche fonti normative (art. 53, comma 2, del Codice), mentre le norme citate dall'Agenzia delle entrate prevedono, in termini assai generici, che gli uffici delle imposte possono "richiedere agli organi ed alle Amministrazioni dello Stato, agli enti pubblici non economici, alle società ed enti di assicurazione ed alle società ed enti che effettuano istituzionalmente riscossioni e pagamenti per conto di terzi la comunicazione, anche in deroga a contrarie disposizioni legislative, statutarie o regolamentari, di dati e notizie relativi a soggetti indicati singolarmente o per categorie" (art. 32, comma 1, n. 5, d.P.R. n. 601/1973 e art. 51, comma 2, n. 5, d.P.R. n. 633/1972). Tant'è che l'art. 19, comma 2, del Codice, relativo alla comunicazione di dati personali tra pp.aa., non si applica al trattamento dei dati da parte delle Forze di polizia, come espressamente stabilito dall'art. 53, comma 2, lett. *a*), del Codice. Del resto, l'acquisizione e la conservazione dei dati della generalità degli "alloggiati" costituiscono una significativa interferenza in particolare con i diritti fondamentali alla protezione dei dati personali (art. 8, Carta diritti fondamentali dell'UE) e alla tutela della vita privata (art. 7, CDFUE e art. 8 Convenzione europea dei diritti dell'uomo) che non può estendersi oltre le previsioni del Tulps. Anche l'art. 9 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, come detto recepita con il decreto legislativo 18 maggio 2018, n. 51, stabilisce che "i dati personali raccolti dalle autorità competenti per le finalità di cui all'art. 1, par. 1, non possono essere trattati per finalità diverse da quelle di cui all'art. 1, par. 1, a meno che tale trattamento non sia autorizzato dal diritto dell'Unione o dello Stato membro" (nota 20 dicembre 2017).

È stato inoltre chiesto al Garante da parte di soggetti privati quali siano le disposizioni da rispettare con particolare riferimento all'obbligo di informativa ed alla necessità di ottenere il consenso dell'interessato, nel caso in cui dati personali di terzi siano oggetto di richieste da parte di autorità di polizia.

Al riguardo è stato rappresentato che, ai sensi dell'art. 13, comma 3, del Codice, l'informativa non debba essere fornita quando la conoscenza, da parte degli interessati, della comunicazione dei loro dati alle autorità di polizia richiedente "può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati". Per quanto riguarda il consenso, questo non è dovuto quando è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria (art. 24, comma 1, lett. *a*), del Codice). Peraltro, l'informativa all'interessato deve essere fornita prima dell'effettuazione di qualsiasi trattamento già al momento dell'acquisizione dei dati o, nel caso in cui i dati personali non sono raccolti presso l'interessato, all'atto della registrazione dei dati oppure, quando è prevista la loro comunicazione, non oltre la prima comunicazione. Pertanto appare opportuno prevedere in via generale, nell'informativa agli interessati, che i loro dati possono essere comunicati alla autorità di pubblica sicurezza ed alle Forze di polizia, nei casi in cui ciò sia previsto dall'ordinamento (nota 19 giugno 2017).

7.6. *Il controllo sul sistema di informazione Schengen*

Il Sistema informativo Schengen (cd. SIS II) svolge un ruolo essenziale nel facilitare la libera circolazione delle persone nello spazio Schengen a seguito dell'eliminazione dei controlli alle frontiere interne. Nel sistema sono contenute segnalazioni sulle persone scomparse, soprattutto minori, e informazioni su determinati beni, quali banconote, automobili, furgoni, armi da fuoco e documenti di identità che potrebbero essere stati rubati, sottratti o smarriti. Lo stesso permette, inoltre, alle autorità nazionali doganali, di polizia e di controllo delle frontiere di scambiarsi agevolmente informazioni sulle persone che potrebbero essere coinvolte in reati gravi.

Come è noto, il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nel SIS II, in virtù delle 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). Al riguardo, condividendo una delle raccomandazioni formulate all'esito della precedente valutazione sull'applicazione dell'*Acquis* di Schengen, si è convenuta la sostituzione del sistema sin qui utilizzato (il quale prevedeva l'invio in copia all'Autorità di ogni comunicazione intercorrente tra Ministero ed interessati) con una più agile modalità consistente nell'invio periodico (trimestrale) da parte del Ministero di *report* statistici, privi di informazioni di natura personale, che contengano dati idonei a monitorare le richieste degli interessati e l'attività di riscontro compiuta dalla Divisione NSIS.

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 pervenute al Garante da autorità nazionali di controllo di altri Stati, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane. Le informazioni sono state comunicate, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni di cui all'art. 62 della decisione 2007/533/GAI del Consiglio e all'art. 46 del regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio.

Come segnalato nella precedente Relazione (p. 157), il rispetto dell'*Acquis* Schengen da parte italiana è stato oggetto nel 2016 della prevista valutazione perio-

dica che ha avuto anche ad oggetto il settore della protezione dei dati personali. In proposito, il Gruppo di valutazione, formato da esperti designati delle Autorità di protezione dati dei Paesi Schengen e coordinato da rappresentanti della Commissione europea, ha redatto il rapporto di valutazione, poi adottato dalla Commissione secondo la procedura prevista dall'art. 14 del regolamento (UE) 1053/2013. Sulla base di alcune carenze dallo stesso individuate, con decisione di esecuzione del 17 febbraio 2017, il Consiglio ha adottato delle raccomandazioni alla luce delle quali l'Italia ha elaborato il piano di azione (ritenuto sufficientemente adeguato dalla Commissione) per correggere le criticità rilevate ed altresì indicato le azioni implementate e le misure già adottate.

La decisione di esecuzione del Consiglio elencava complessivamente per l'Italia 27 raccomandazioni, tra l'altro riguardanti lo svolgimento dell'*audit* sui processi operativi svolti in ambiente SIS II, conformemente agli *standard* internazionali.

Alcune raccomandazioni hanno riguardato anche il Garante, in qualità di autorità competente per la supervisione nazionale del Sistema informativo Schengen II (SIS II) e del Sistema informativo visti (VIS, istituito con la Decisione del Consiglio dell'Unione europea 2004/512/CE del 8 giugno 2004), in relazione alle attività di verifica e controllo svolte con riferimento alla legittimità del trattamento dei dati operato dai due titolari del trattamento dei sistemi in questione (Ministero dell'interno e Ministero degli esteri).

In tale quadro, in esito ad alcuni incontri interlocutori, è stato inviato al Ministero dell'interno un apposito questionario. La valutazione delle risposte del Ministero è stata completata e sono in corso ulteriori attività di verifica circa la legittimità del trattamento dei dati, all'esito delle quali verrà impostato lo svolgimento dei successivi controlli.

In conformità al piano d'azione, l'Ufficio ha provveduto inoltre a migliorare alcuni aspetti relativi alla comunicazione delle informazioni sul sito istituzionale dell'Autorità, nonché a portare a conclusione le attività di verifica sul trattamento dei dati personali effettuati nelle procedure di rilascio dei visti e nel VIS.

Tali attività, svolte nell'ambito degli specifici obblighi di vigilanza previsti dall'art. 41 del regolamento (CE) n. 767/2008 – in base al quale le autorità di controllo nazionali (che esercitano autonomamente i poteri di controllo sulla legittimità del trattamento dei dati personali registrati nel VIS), almeno ogni quattro anni, svolgono un'attività di controllo (*audit*) sulle operazioni di trattamento dei dati del sistema nazionale, in conformità alle pertinenti norme di revisione internazionali – sono consistite anche in alcune verifiche *in loco*, presso il Ministero degli affari esteri e della cooperazione internazionale, in relazione alla gestione, anche per i profili della sicurezza dei dati, del Sistema informativo nazionale, nonché presso una sede consolare estera, dove è stata verificata l'operatività dell'ufficio visti consolare e di una società *outsourcer* (ESP) locale.

8 L'attività giornalistica

Alle varie forme di manifestazione del pensiero, sia attraverso i *media* tradizionali e, sempre più spesso, in relazione alla diffusione di informazioni personali in internet, l'Autorità continua a dedicare particolare attenzione al fine di assicurare uno *standard* elevato di tutela dei diritti fondamentali degli interessati. Tale cura si manifesta in larga misura nelle frequenti interlocuzioni dell'Ufficio con le varie testate giornalistiche (nazionali o locali) e i *blog* di volta in volta oggetto di segnalazione cui, di regola, senza la necessità di adozione di provvedimenti da parte del Garante, hanno fatto seguito interventi spontanei da parte dei soggetti chiamati in causa che hanno provveduto alla rimozione o rimodulazione del contenuto di articoli contenenti informazioni (e non di rado anche immagini a corredo degli stessi) eccedenti rispetto al perseguimento della finalità informativa.

In qualche occasione, tuttavia, il Garante ha assunto decisioni puntuali sui casi portati alla sua attenzione e, in più di una circostanza, a seguito dell'esercizio dei diritti di cui all'art. 7 del Codice da parte degli interessati, si è pronunciato in sede di ricorso da parte degli stessi, specie con riguardo ai casi nei quali è stata richiesta la deindicizzazione di informazioni personali (in merito si rinvia al cap. 19).

Consiglio nazionale dell'Ordine dei giornalisti

Né la cura per le tematiche in parola si è esaurita nell'attività provvedimentale da parte dell'Autorità. Dopo aver (ulteriormente) sollecitato nel 2016 un'opportuna (e sempre più urgente) opera di aggiornamento del codice di deontologia, data la rilevanza assunta dalla dimensione digitale ed il crescente impatto di internet e dei *social network* sui diritti della persona (cfr. nota del Presidente 21 aprile 2016, ricordata nella Relazione 2016, p. 76, rimasta tuttavia senza ricadute concrete), anche nel 2017 il Garante è tornato a sollecitare l'Ordine dei giornalisti, richiamandone l'attenzione sull'applicazione dei principi ormai consolidati contenuti nel codice di deontologia del 1998. In particolare ha invocato un più attento rispetto del principio di essenzialità dell'informazione a fronte delle descrizioni particolareggiate su fatti e persone riscontrate nella pubblicazione di notizie concernenti episodi delittuosi, riguardanti anche casi di violenza sessuale, ovvero con riguardo alla diffusione di informazioni tratte da atti di indagine, evidenziando l'ulteriore pregiudizio arrecato agli interessati dalla presenza e permanenza in rete di notizie che li riguardano. L'Autorità ha altresì invitato l'Ordine a garantire un'informazione più rispettosa del principio di non discriminazione (in particolare su base etnica) e più attenta ai diritti dei minori coinvolti in fatti di cronaca (nota del Presidente 21settembre 2017).

Gruppo di lavoro sulla "Tutela dei minorenni nel mondo della comunicazione"

Tema, quello della protezione dei minori, sul quale, non a caso, come già riferito nella Relazione 2016 (cfr. p. 76), l'attività istituzionale dell'Autorità ha trovato ulteriore occasione di manifestazione nella partecipazione dell'Ufficio al Gruppo di lavoro della Consulta nazionale delle associazioni e delle organizzazioni "Tutela dei minorenni nel mondo della comunicazione" istituito presso l'Autorità garante per l'infanzia e l'adolescenza (che ha coinvolto varie competenze operanti in ambiti istituzionali e nelle realtà associative), con l'obiettivo di approfondire i temi della tutela del minore rispetto alle varie dimensioni della comunicazione (carta stampata, *media* tradizionali, dimensione digitale e *social network*); il documento elaborato dal Gruppo di lavoro è stato pubblicato sul sito web istituzionale dell'Autorità garante per l'infanzia e l'adolescenza con il titolo "La tutela dei minorenni nel mondo della comunicazione".

8.1. *I minori*

Con riguardo alla protezione dei diritti dei minori – considerato che un'irrispettosa diffusione dei dati agli stessi riferiti può determinare ripercussioni gravi sulla riservatezza e sulla dignità individuale (in taluni casi compromettendo l'armonico sviluppo della personalità dell'interessato) – merita di essere qui ricordato il provvedimento 16 novembre 2017, n. 478 (doc. web n. 7354837) adottato nei confronti di una testata giornalistica al fine di tutelare il diritto all'immagine e all'identità personale di una minore. Oggetto della segnalazione (formulata dal padre) è stata una foto di una bambina, ritratta vestita da sposa nell'atto di infilare un anello nuziale nella mano di un adulto, pubblicata sulla pagina web (oltre che nella pagina Facebook) di una testata *online*. La foto della minore, ritratta in abito matrimoniale per una campagna di sensibilizzazione contro la pratica delle spose bambine promossa da una Ong internazionale, era stata invece pubblicata a corredo di un articolo che riguardava altra minore ridotta in schiavitù dal padre e promessa in sposa ad un connazionale dietro pagamento di una somma di denaro.

Secondo il Garante, la testata *online* ha quindi impropriamente utilizzato la foto, tratta da tutt'altro contesto, in modo da indurre i lettori a ritenere che la minore ritratta fosse la vera protagonista del fatto di cronaca. L'associazione della fotografia della bambina protagonista della campagna di sensibilizzazione, figlia del segnalante, ha configurato un trattamento illecito di dati personali atteso che l'accostamento, dell'immagine al fatto di cronaca è lesivo del diritto all'identità personale della minore (artt. 2, 11 e 137 del Codice) e può arrecare un danno alla bambina fotografata, la cui immagine era stata diffusa con finalità del tutto diverse. Né la testata aveva adottato alcun accorgimento per prevenire l'identificazione della minore (ad es., pixelandone il volto), misura che, se richiesta (in astratto) rispetto alla eventuale diffusione della foto della vera protagonista della vicenda (art. 7 del codice deontologico dei giornalisti e Carta di Treviso), a maggior ragione si sarebbe dovuta adottare nel caso considerato, che nulla aveva a che vedere con i fatti di cronaca riportati nell'articolo. All'editore della testata, che nel corso dell'istruttoria ha rimosso la fotografia dal sito, l'Autorità ha prescritto di adottare le misure necessarie affinché l'immagine non venga ulteriormente utilizzata in violazione del diritto all'identità personale della bambina.

8.2. *La cronaca giudiziaria*

Tra i casi portati all'attenzione del Garante, alcune peculiarità presenta quello oggetto di un reclamo con il quale si lamentava la violazione del Codice in relazione ad alcuni articoli pubblicati, anche nell'edizione *online*, da un quotidiano a tiratura nazionale (ancorché nelle pagine della cronaca locale), aventi ad oggetto la notizia di un procedimento penale a carico del reclamante quale presunto responsabile della sottrazione di cospicue somme di denaro dalle casse delle sale da gioco presso cui lavorava (provv. 12 ottobre 2017, n. 409, doc. web n. 7273804). Rispetto a tale vicenda il Garante ha ritenuto sussistente un interesse pubblico tale da giustificare le notizie di stampa in ragione delle attività e dei luoghi interessati (le sale da gioco, caratterizzate di regola da un notevole afflusso di pubblico e da una circolazione significativa di denaro) e dei fatti narrati (l'acquisizione indebita di denaro dalle casse delle predette sale), per i quali era altresì pendente un procedimento giudiziario. L'interesse pubblico alla conoscenza dei fatti in questione è stato fondato anche su ulteriori elementi caratterizzanti la vicenda, in considerazione sia della qualità di

incaricato di pubblico servizio (che sarebbe rivestita dal reclamante, in virtù della quale, stando alle notizie di stampa, nei suoi confronti potrebbero essere ipotizzati una serie di gravi reati), sia del danno rilevante che la condotta del reclamante avrebbe arrecato all'erario a causa del mancato versamento degli introiti delle sale gioco in violazione di quanto previsto dalla disciplina di settore. Peraltro, come si evince da alcune foto poste a corredo di un articolo, la vicenda ha avuto particolare evidenza a livello locale, dove non sono mancate manifestazioni pubbliche di preoccupazione e di malcontento da parte dei dipendenti di alcune delle sale da gioco coinvolte nei fatti.

Alla luce di questi complessivi elementi, la scelta effettuata dalla testata di pubblicare anche i dati identificativi del reclamante, quale persona verso cui si sono rivolte le indagini, non è stata reputata contraria al principio di essenzialità dell'informazione, anche sulla scorta di alcune precedenti decisioni del Garante che in più occasioni ha affermato che la pubblicazione dei nomi di persone interessate da un procedimento penale in qualità di indagati, imputati o condannati non è preclusa dall'ordinamento vigente e va piuttosto inquadrata nell'ambito delle garanzie volte ad assicurare trasparenza e controllo da parte della collettività sull'attività di giustizia (in tal senso cfr. provv.ti 24 novembre 2016, n. 489, doc. web n. 5905569; 21 aprile 2016, n. 187, doc. web n. 5146073; in tema cfr. anche il documento del Garante del 6 maggio 2004, *Privacy* e giornalismo. Alcuni chiarimenti in risposta a quesiti dell'Ordine dei giornalisti, doc. web n. 1007634; tale orientamento è altresì riscontrabile in Cass. civ., sez. I, 19 marzo 2008, n. 7261, Cass. civ., sez. III, 9 gennaio 2014, n. 194). Né si è ritenuto costituire una violazione del principio di essenzialità dell'informazione il riferimento contenuto negli articoli alla presunta patologia del reclamante (la ludopatia), atteso che tale circostanza risulta essere emersa quale elemento fondante della vicenda (ed indicata come elemento condizionante dell'operato del reclamante) e non è stata comunque corredata da informazioni analitiche relative alla salute del reclamante medesimo o altrimenti lesive della sua dignità (cfr. artt. 5 e 10 codice di deontologia).

Nel ritenere infondato il reclamo, il Garante ha comunque rappresentato che ciò non preclude al reclamante, sussistendone i presupposti e alla luce dei futuri sviluppi giudiziari, di chiedere l'aggiornamento della notizia (cfr. art. 7, comma 3, lett. *a*), del Codice; Cass. civ, sez. III, 5 aprile 2012, n. 5525), ovvero l'integrazione degli elementi che riguardano la vicenda, fornendo i necessari elementi a supporto delle pretese fatte valere (cfr. in merito Cass. civ., sez. III, 30 dicembre 2014, n. 27535, Cass. civ., sez. II, 5 aprile 2012, n. 5525 e provv. 20 ottobre 2016, n. 430, doc. web n. 5690019).

8.3. *La diffusione delle informazioni* online

In altra occasione è stato lamentato da parte di alcuni attivisti del Movimento 5 Stelle la diffusione del contenuto parziale di alcune *e-mail*, scambiate all'interno di un gruppo chiuso di utenti, nell'ambito dell'articolo pubblicato su una testata nazionale (e presente altresì sulla versione *online* della stessa), poi ripreso da molti siti web (provv. 2 febbraio 2017, n. 36, doc. web n. 6118783). Muovendo dall'assunto che il giornalista può diffondere dati personali, anche sensibili, senza il consenso degli interessati purché nei limiti posti al diritto di cronaca e, in particolare, nel rispetto del requisito "dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico" (art. 137, comma 3, del Codice), non si è ritenuto illecito il contenuto dell'articolo portato all'attenzione del Garante. Con riferimento al profilo

della liceità della raccolta delle *e-mail* scambiate all'interno di "Google Groups", non sono emersi dall'istruttoria elementi tali da comprovare un'acquisizione illecita delle *e-mail* da parte del giornalista. Per quanto riguarda la legittimità del successivo trattamento per finalità giornalistiche, l'art. 93, l. 22 aprile 1941, n. 633, applicabile in virtù del richiamo contenuto nell'art. 184, comma 3, del Codice, prevede che la corrispondenza possa essere pubblicata, riprodotta od in qualunque modo portata alla conoscenza del pubblico solo con il consenso dell'autore e del destinatario, allorché la stessa abbia "carattere confidenziale" o si riferisca "alla intimità della vita privata". Nel caso di specie le *e-mail* pubblicate contenevano, tuttavia, valutazioni di carattere esclusivamente politico e non sono state quindi considerate attinenti all'intimità della vita privata. Quanto, invece, al loro eventuale carattere confidenziale, sulla scorta di giurisprudenza in materia, si è ritenuto che le modalità di scambio delle informazioni tra i reclamanti, per il tramite di una *mailing list*, non potesse in alcun modo definirsi confidenziale, avuto riguardo al cospicuo numero dei soggetti che vi facevano parte ed all'eterogeneità degli stessi (che comprendevano, oltre ai 14 reclamanti, anche ex consiglieri comunali militanti nel medesimo Movimento, alcuni parlamentari ed alcuni operatori privati del settore urbanistico), circostanze che hanno determinato il Garante a ritenere del tutto assente ogni ragionevole aspettativa in ordine alla effettiva riservatezza del contenuto delle conversazioni tenute all'interno del gruppo.

Le parti delle *e-mail* riportate nell'articolo rispondevano altresì al requisito della "essenzialità dell'informazione riguardo a fatti di interesse pubblico" (art. 137, comma 3, del Codice), essendo afferenti alle dinamiche interne al Movimento, attore politico rilevante nel panorama nazionale, anche in considerazione dell'intervallo temporale in cui le vicende si sono svolte (alla vigilia delle elezioni amministrative a Roma); né, infine, è stata ritenuta sussistente una violazione dei dati personali sensibili riferiti ai segnalanti, risultando comprovata la militanza e la partecipazione attiva degli stessi per il Movimento.

9 Il cyberbullismo

Con l'entrata in vigore della legge 29 maggio 2017, n. 71, contenente "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" (sulla quale v. par. 2.1.1), sono stati affidati al Garante compiti specifici in questa delicata materia. In particolare l'art. 2 prevede che qualora un minore sia vittima di un atto riconducibile a tale condotta ("qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti *online* aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo") il minore stesso, se ultra quattordicenne, o chi esercita la responsabilità genitoriale, dopo essersi rivolto (infruttuosamente) al titolare del trattamento o al gestore del sito o del *social media* per ottenere tutela ("l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet"), può rivolgersi al Garante "il quale, entro quarantotto ore dal ricevimento della richiesta, provvede ai sensi degli articoli 143 e 144 del […] decreto legislativo 30 giugno 2003, n. 196".

Per dare attuazione alle nuove attribuzioni rimesse al Garante, è stata realizzata sul sito web dell'Autorità una sezione dedicata al tema nella quale, per agevolare il compito dei soggetti legittimati a segnalare episodi di cyberbullismo, è reperibile un'infografica sul fenomeno, un modello per la segnalazione dei casi all'Autorità e una casella di posta elettronica *ad hoc* (cyberbullismo@gpdp.it).

Le fattispecie segnalate al Garante, 17 nel periodo luglio-dicembre 2017, rispetto alle quali l'Autorità si è attivata nei tempi previsi dal legislatore, hanno riguardato ipotesi tra loro diverse (creazione di falsi profili, talvolta finalizzati allo scambio di messaggi a sfondo sessuale, diffusione di messaggi offensivi e denigratori e/o di fotografie scattate in ambito privato) e interessato diversi *social media* localizzati in ambito europeo ed extraeuropeo. Di questi, per larga parta dei casi si è definita la segnalazione con la rimozione del contenuto denunciato (con l'avvio dell'istruttoria da parte dell'Ufficio o per autonoma iniziativa del gestore del sito). Nei casi restanti, talora non è stata ulteriormente coltivata la segnalazione da parte degli interessati o non si sono ritenuti sussistenti gli estremi per ricondurre la fattispecie segnalata all'interno dei confini della disciplina del cyberbullismo (talvolta anche in ragione della genericità della segnalazione). In tutti i casi è stato comunque fornito riscontro ai segnalanti e, in talune fattispecie, la segnalazione è stata inoltrata alla Polizia postale.

Criticità sono state riscontrate dall'Ufficio in particolare nei casi relativi a siti gestiti da soggetti collocati fuori dal territorio europeo.

Con riguardo alla materia considerata, merita ricordare che, a seguito dell'entrata in vigore della menzionata legge n. 71/2017 è stato altresì istituito, con il d.P.C.M. 26 ottobre 2017, n. 2566, il Tavolo tecnico interistituzionale, il cui coordinamento è affidato al Ministero dell'istruzione, dell'università e della ricerca, riunitosi, con la partecipazione di personale dell'Autorità, il 6 febbraio 2018.

Inoltre, il 28 dicembre 2017, il Garante ha sottoscritto un protocollo di intesa con la Polizia postale ai fini di cooperazione e supporto nello svolgimento dell'attività di prevenzione e contrasto del cyberbullismo.

10 *Marketing*, profilazione e trattamento dei dati personali

10.1. *Verifiche preliminari*

Con provvedimento 12 ottobre 2017, n. 410 (doc. web n. 7297879) il Garante, nel valutare l'istanza di verifica preliminare presentata da una società che opera nel settore della grande distribuzione con oltre 60 ipermercati, ha autorizzato il prolungamento dei tempi di conservazione dei dati relativi alla clientela per finalità di promozione commerciale profilata fino a 24 mesi (anziché 12 mesi, come previsto dal provv. 24 febbraio 2005 in materia di carte di fidelizzazione, doc. web n. 1103045). Sulla base di quanto rappresentato dalla società infatti, nella congiuntura economica attuale, caratterizzata da una significativa contrazione dei consumi e dalla forte competitività tra gli operatori, si pone l'esigenza di cogliere i *trend* di mercato in tempi molto ristretti, proponendo offerte mirate e che, al contempo, incontrino la domanda secondo una tempistica puntuale. Poiché alcune tipologie di acquisti sono di carattere stagionale (articoli natalizi, pasquali, per il mare, per il giardinaggio, per la scuola, ecc.) e tendono ad essere effettuati solo in prossimità dell'evento, la limitazione temporale di 12 mesi stabilita nell'anzidetto provvedimento del Garante determinerebbe, per gli operatori di settore, un vuoto informativo proprio nel momento in cui i dati necessitano di essere analizzati. La tempistica più ampia, autorizzata dall'Autorità, consente quindi alla società istante di organizzare in modo più mirato le politiche di vendita e, al tempo stesso, di gestire in modo più efficiente gli inventari e gli approvvigionamenti con conseguenti effetti favorevoli sia per la società, in termini di contrazione dei costi, sia per i clienti che potranno avvantaggiarsi dei prodotti in offerta. Con il medesimo provvedimento l'Autorità ha inoltre esteso l'autorizzazione in questione ai diversi titolari del trattamento che operino nel settore della grande distribuzione organizzata, a condizione che le modalità del trattamento siano analoghe a quelle stabilite nel provvedimento (tra cui, in particolare, la cancellazione automatica o la trasformazione in forma anonima dei dati alla scadenza dei 24 mesi, un'adeguata modulistica per la raccolta del consenso e un'informativa specifica) e che siano adottati gli accorgimenti prescritti nel provvedimento generale del 24 febbraio 2005.

Beni di lusso

Anche nel 2017 sono pervenute numerose istanze di verifica preliminare da società operanti nel settore dei beni di lusso, finalizzate ad una conservazione dei dati della propria clientela, per finalità di profilazione e *marketing*, per intervalli temporali superiori a quelli stabiliti dal Garante nel provvedimento del 24 febbraio 2005, parte delle quali sono state definite con provvedimento collegiale.

Coerentemente all'indirizzo assunto negli anni passati (e del quale si è dato conto nelle precedenti Relazioni), in ragione delle peculiarità dei settori merceologici nei quali le società istanti operano, è stato ritenuto congruo un periodo di conservazione dei dati per le menzionate finalità, in presenza di un consenso degli interessati (pienamente informato e distintamente riferito a ciascuna di esse), pari a sette anni; ciò considerando che i beni acquistati formano oggetto di acquisto saltuariamente, sicché un ridotto periodo di conservazione comprometterebbe un efficace perseguimento delle finalità perseguite (provv.ti 9 marzo 2017, n. 128, doc. web n. 6342201; 11 maggio 2017, n. 227, doc. web n. 6495144; 5 luglio 2017, n. 304, doc. web n. 6844421).

10.2. *Marketing*

Come già indicato nella Relazione 2016 (cfr. p. 83 ss.), le segnalazioni pervenute in materia di *marketing*, con assoluta prevalenza di quelle riferite al cd. *telemarketing* selvaggio, quindi all'invio di comunicazioni commerciali via *e-mail* o sms, (anche solo) dal punto di vista quantitativo continuano a comporre, anche per il 2017, il "carico" assolutamente prevalente dell'Autorità (v. anche par. 23.5). Ancorché con qualche flessione rispetto al dato numerico registrato in passato, esse rimangono, con particolare riguardo all'ambito del *telemarketing*, alcune migliaia (per un'analisi di dettaglio v. sez. IV, tab. 10), con una tendenza che, specie con riguardo a taluni operatori, non sembra dare segnali tangibili di flessione.

Dall'analisi delle segnalazioni pervenute è dato desumere che esse continuano ad interessare sia gli abbonati iscritti nel Registro pubblico delle opposizioni (Rpo) – circostanza dalla quale si devono quindi desumere comportamenti tutt'altro che virtuosi da parte di non pochi soggetti operanti nella (non di rado lunga) filiera del *telemarketing*, che dal committente della campagna promozionale si snoda fino all'ultimo anello della stessa, l'operatore che materialmente effettua la chiamata –, sia i titolari di numerazioni (residenziali e, sempre più spesso, mobili) non pubblicate su elenchi telefonici (cd. numerazioni riservate). I settori merceologici nei quali operano i committenti oggetto di segnalazione continuano ad essere occupati principalmente dalle società che offrono servizi di comunicazione elettronica e dalle *utilities* (in particolare gli operatori del settore energetico), con una differenziata consistenza numerica delle segnalazioni rispetto a ciascuno degli operatori; non di rado modalità particolarmente aggressive (oltre che la mancata identificazione del committente) vengono segnalate rispetto a chiamate promozionali, per lo più effettuate da *call center* stabiliti al di fuori dei confini nazionali, nel settore finanziario e valutario (aventi genericamente a contenuto "Forex" o "Trading").

Peraltro, in termini generali, sono frequenti le telefonate promozionali indesiderate rispetto alle quali se ne lamenta l'esecuzione da parte di *call center* stabiliti al di fuori del territorio nazionale. Non pare infine venir meno il fenomeno delle telefonate effettuate, in violazione di legge, con numerazione chiamante oscurata.

Sotto diverso profilo, persistono i casi nei quali viene segnalato il mancato o tardivo riscontro con riguardo all'esercizio dei diritti degli interessati da parte degli operatori economici nel cui interesse si lamentano essere effettuate le comunicazioni promozionali – fenomeno già segnalato nella Relazione 2016, p. 85 (e, tra l'altro, oggetto del provv. 21 settembre 2016, n. 368, doc. web n. 5774043; v. altresì provv.ti 22 giugno 2016, n. 275, doc. web n. 5255159, punti 7.2 e 7.3; 21 luglio 2016, n. 317, doc. web n. 5436585) e talora emerso anche nell'ambito di decisioni adottate su ricorso (cfr., ad es., provv.ti 16 marzo 2017, n. 149, doc. web n. 6503967; 6 aprile 2017, n. 184, doc. web n. 654439; 31 maggio 2017, n. 260, doc. web n. 6608298; 23 novembre 2017, n. 501, doc. web n. 7666773) –, al di là del (solo) diritto di opposizione all'ulteriore trattamento dei dati per finalità di *marketing*, e nei quali viene stigmatizzata la carenza di riscontro rispetto alle necessarie indicazioni, ad esempio, circa l'origine dei dati, elemento conoscitivo imprescindibile al fine di consentire all'interessato di risalire agli archivi che stanno a monte delle comunicazioni telefoniche indesiderate. Per tale ragione, nel 2017, sia in occasione delle verifiche effettuate *in loco*, sia con istruttorie documentali, l'Autorità ha moltiplicato le attività di controllo volte ad accertare la fondatezza delle segnalate carenze.

Il riscontro ai segnalanti

Sotto diverso profilo, ma si tratta di attività parimenti significativa, l'Autorità, riformulate le FAQ presenti sul proprio sito web (doc. web n. 1794339), ha continuato a dare riscontro individualizzato a larga parte delle (migliaia di) segnalazioni

pervenute (sovente da parte di segnalanti che reiteratamente lamentano la persistenza dei contatti indesiderati, nonostante l'esercizio del diritto di opposizione o l'iscrizione della propria numerazione nel Rpo), anzitutto al fine di fornire informazioni corrette sugli strumenti messi a disposizione dall'ordinamento a vantaggio degli interessati per prevenire od opporsi alle telefonate indesiderate (esercitando i diritti di cui all'art. 7 del Codice anche avvalendosi del modello predisposto dall'Autorità: cfr. doc. web n. 1089924). In questa prospettiva, nelle comunicazioni individuali si sono invitati i segnalanti a non escludere la possibilità, quantomeno in taluni casi, della liceità del contattato commerciale sulla base di un consenso prestato, anche (e spesso) per inavvertenza, a vantaggio del medesimo operatore economico nel cui interesse si è stati contattati (come, in occasione dell'acquisto di beni o servizi forniti) o di terzi (ad es., partecipando a concorsi a premi, o autorizzando tali usi su siti web di natura più varia per l'utilizzo, magari senza corrispettivo, di alcuni servizi); sulla base di tale consenso – talora illegittimamente acquisito, come nei casi di cd. consenso obbligato (fenomeno assolutamente persistente, ancorché contrastato dal Garante: cfr. par. 10.4) – le numerazioni telefoniche formano oggetto di comunicazione a (più) operatori economici (anche in tempi successivi) e quindi alimentano il flusso dei contatti promozionali, con un processo che a fatica può essere interrotto.

Muovendo da tali segnalazioni (per lo più valutate nel loro insieme e talora prese anche in considerazione individualmente per verifiche a campione), nel corso dell'anno si sono svolte numerose verifiche *in loco* presso una pluralità di *call center* situati sul territorio nazionale, facenti per lo più capo a operatori economici costituiti nella forma di società a responsabilità limitata in forma semplificata (con capitale sociale assai modesto, di regola non superiore ai 1000 euro) che non di rado hanno fatto emergere aree di inosservanza degli obblighi derivanti dalla disciplina di protezione dei dati personali e che, in qualche caso, hanno disvelato un utilizzo ripetuto, nelle attività di contatto, di consistenti basi di dati di dubbia origine.

Al di là delle difficoltà in concreto incontrate dall'Ufficio per individuare i *call center* oggetto di verifica – in qualche caso la numerazione VoIP utilizzata è risultata intestata a soggetti che hanno denunciato alle competenti Autorità la propria estraneità all'utenza di cui risultavano intestatari – e finanche nello svolgimento delle attività di controllo (in ragione del grado di collaborazione prestato al personale incaricato degli accertamenti), il concorrere delle circostanze qui rappresentate appalesa l'insufficienza del quadro normativo vigente e il limitato effetto deterrente derivante dalle (pur significative, in astratto) sanzioni amministrative di natura pecuniaria rispetto a questa tipologia di operatori economici. A tacer del fatto, peraltro, che pure nel caso in cui tali rimedi trovino in concreto applicazione all'esito dei procedimenti attivati avanti al Garante, nei fatti la natura dematerializzata delle informazioni concernenti le numerazioni utilizzate consente a quanti intenzionalmente vogliono sottrarsi alle regole vigenti (peraltro a danno non solo degli interessati, ma anche degli operatori economici che tali regole intendono rispettare) di farlo, duplicando e riutilizzando (o trasferendo) agevolmente il patrimonio informativo – non di rado rilevantissimo (provv.ti 15 giugno 2017, n. 268, doc. web n. 6629169 e 30 marzo 2017, n. 168, doc. web n. 6393365, di seguito illustrati, nei quali le verifiche hanno consentito di appurare il trattamento illecito di milioni di utenze telefoniche) – accumulato nel tempo o del quale, con le più varie (non sempre lecite) modalità, sono venuti a disposizione.

A valle di queste multiformi attività, il Garante, stigmatizzando (ripetutamente, anche nei confronti degli organi di informazione) il cd. *telemarketing* selvaggio quale "fenomeno distorsivo delle comunicazioni commerciali", ha confermato,

nelle sedi istituzionali, che lo stesso "è, da tempo, all'attenzione dell'Autorità e oggetto di un'attività di deciso contrasto" (cfr. audizione informale del Presidente del Garante – d.d.l. 2452 e 2545, concernenti modifiche del Registro delle opposizioni e contrasto al cd. *telemarketing* selvaggio, presso la 8ª Commissione permanente – Lavori pubblici, comunicazioni – del Senato della Repubblica, 16 novembre 2016, doc. web n. 5661956). Del pari il Garante si è pronunciato a favore della modifica del Rpo, al fine di consentire l'iscrizione nello stesso anche di numerazioni non presenti negli elenchi pubblici, e dell'introduzione di una specifica previsione affinché "l'iscrizione al Registro comporti la cancellazione automatica di tutti i consensi dati precedentemente dall'interessato per le telefonate commerciali", determinazione questa avente "il significato di una procedura aggiuntiva di revoca del consenso precedentemente rilasciato" (cfr. audizione informale cit.).

Modifiche normative in materia di Rpo e *telemarketing*

In questa direzione, con l'intento di favorire un più efficace contrasto del *telemarketing* selvaggio, è da ultimo intervenuto il legislatore, con la legge 11 gennaio 2018, n. 5, "Nuove disposizioni in materia di iscrizione e funzionamento del Registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato" (v. par. 2.1.1). Tra le principali innovazioni legislative – talune delle quali troveranno applicazione a seguito dell'emanazione del regolamento attuativo previsto dall'art. 1, comma 15 della legge – vanno infatti segnalate: l'estensione della possibilità di iscrizione nel Rpo a tutte le numerazioni, residenziali e mobili, a prescindere dalla loro presenza negli elenchi telefonici pubblici (cd. riservati) (art. 1, comma 2); la previsione secondo la quale, per effetto dell'iscrizione nel Registro, verranno meno gli effetti del consenso precedentemente prestati dagli interessati per finalità pubblicitarie (art. 1, comma 5); l'obbligo per i *call center* di effettuare le chiamate con il numero identificabile (e ricontattabile) o, in alternativa, l'utilizzo di un prefisso specifico che consenta al destinatario della chiamata di desumerne la natura promozionale; l'obbligo per i *call center* di verificare presso il Rpo, almeno una volta al mese, che le numerazioni che intendono chiamare per fini pubblicitari non siano iscritte nel Registro stesso; il potenziamento del quadro sanzionatorio.

Rpo e posta cartacea

Con provvedimento 29 dicembre 2017, n. 565 (doc. web n. 7656748) è stato espresso dal Garante il richiesto parere sullo schema di decreto del Presidente della Repubblica, recante "Modifiche al regolamento di cui al decreto del Presidente della Repubblica 7 settembre 2010, n. 178, ai sensi dell'art. 1, comma 54, della legge 4 agosto 2017, n. 124 – Legge annuale per il mercato e la concorrenza, in materia di Registro pubblico delle opposizioni" – evidenziando anzitutto la necessità di alcune integrazioni al testo, per renderlo coerente con il dichiarato intento di estendere la disciplina vigente relativa al Rpo anche alla "posta cartacea" o al trattamento dei dati personali relativi "agli indirizzi postali" degli "abbonati"; il Garante ha altresì evidenziato l'opportunità di porre in essere campagne informative per pubblicizzare il più ampio ambito di operatività del Rpo a seguito delle innovazioni introdotte, coerentemente a quanto già previsto all'art. 11, d.P.R. n. 178/2010, nonché di introdurre una misura transitoria per consentire l'utilizzo degli indirizzi presenti negli elenchi pubblici per finalità di *marketing* solo dopo il decorso di un termine congruo dall'entrata in vigore delle modifiche regolamentari contenute nello schema; tale intervallo temporale (specie ove associato ad un'efficace campagna di comunicazione istituzionale) consentirebbe, infatti, a quanti intendano opporsi all'utilizzo degli indirizzi presenti negli elenchi pubblici, di provvedervi tempestivamente (prevenendo

così ogni indesiderato trattamento dei propri recapiti per finalità commerciali) (cfr. par. 3.3.1).

10.3. *Telefonate indesiderate a contenuto promozionale: i controlli*

Le verifiche *in loco*

La persistenza del cd. *telemarketing* selvaggio nel tempo (con polarizzazione su alcuni degli operatori oggetto di numerose e ripetute segnalazioni), il percepito fastidio (e, in taluni casi, l'esasperazione) di quanti effettuano le segnalazioni all'Autorità (e, nonostante la loro numerosità, si tratta solo di una goccia nell'oceano, anche alla luce di quanto emerge dagli accertamenti effettuati), la crescente attenzione dedicata ad esso dagli organi di stampa – anche per altri fattori (primo fra tutti la crisi occupazionale che interessa il settore dei *call center*) – sono le ragioni che hanno condotto ad un impiego (che ben può essere definito straordinario) delle risorse a disposizione dell'Autorità in questo contesto, con l'inserimento del *telemarketing*, anche nel 2017, tra i settori per i quali è stata pianificata l'attività ispettiva di iniziativa curata dall'Ufficio per mezzo della Guardia di finanza (cfr. deliberazione 27 luglio 2017, n. 357, doc. web n. 6955256). Tale accentuato impegno ha comportato un incremento dell'attività di controllo da parte dell'Autorità, con verifiche ispettive *in loco* sia presso i principali committenti, sia presso alcuni dei *call center* che l'attività istruttoria curata dall'Ufficio ha consentito di individuare. Verifiche che solo in parte è stato possibile definire nel 2017 (v. *infra*), atteso che non pochi accertamenti si sono prolungati nel corso dell'anno e potranno formare oggetto di compiuta valutazione nel 2018.

Cooperazione con l'Autorità di protezione dei dati albanese

Menzione particolare merita, entro questa cornice, il consolidamento dei rapporti di collaborazione con l'Autorità di protezione dei dati albanese (fondati nel protocollo di cooperazione del 15 febbraio 2015), concretizzatosi in una prima visita a Tirana di personale dell'Autorità, con scambio di informazioni rispetto al fenomeno del cd. *telemarketing* selvaggio e alle modalità di contrasto dello stesso, conclusasi con un *workshop* aperto agli operatori del settore stabiliti in territorio albanese; quindi nello svolgimento di alcune attività ispettive da parte dell'Autorità albanese con la partecipazione di personale dell'Ufficio, mirate ad effettuare controlli su un campione (necessariamente limitato) degli operatori che, in base agli elementi precedentemente elaborati dall'Ufficio, risultavano effettuare chiamate dirette a soggetti residenti in Italia. Alla luce di questa prima esperienza, svoltasi con la piena collaborazione dell'Autorità albanese (e sulla base dei poteri alla stessa attribuiti dalla legislazione nazionale), persistendo il fenomeno del *telemarketing* effettuato da operatori stabiliti sul territorio albanese, ulteriori verifiche mirate potranno richiedere un ulteriore affinamento degli strumenti di accertamento e reazione che i diversi ordinamenti giuridici mettono a disposizione delle Autorità di controllo ed una riflessione sull'eventuale necessità di un rafforzamento degli stessi.

Numerazioni ed indirizzi *e-mail* reperiti in internet

Quanto sopra rappresentato in termini generali trova conferma in alcune delle fattispecie che hanno formato oggetto di valutazione da parte del Garante. Così gli accertamenti effettuati dall'Ufficio in collaborazione con il Nucleo speciale *privacy* hanno consentito di appurare che, per acquisire nuovi clienti e promuovere i propri prodotti, una società, attiva nell'offerta di servizi in internet (costruzione e gestione di siti web, posizionamento nei motori di ricerca, vendita di spazi pubblicitari e attività di *social media marketing*), contattava telefonicamente utenze reperite in rete, in genere ricercando i numeri di telefono di liberi professionisti e di imprese individuali presenti nell'area "contatti" dei siti web visionati. Un trattamento ritenuto dal Garante (già in

passato) in violazione della disciplina di protezione dei dati personali, in quanto effettuato in assenza della previa acquisizione del consenso informato degli interessati e, più radicalmente, ponendosi in violazione del principio di finalità; a quest'ultimo riguardo si è ribadito che i numeri di telefono presenti in internet, seppur liberamente conoscibili da chiunque, non possono tuttavia essere legittimamente utilizzati per finalità (come il *marketing*) diverse e non compatibili rispetto a quelle che ne hanno determinato la pubblicazione *online* (provv. 12 gennaio 2017, n. 4, doc. web n. 5986406).

Consenso "unico"

Nell'ambito dello stesso provvedimento, il Garante ha altresì vietato alla società l'uso dei dati per finalità promozionali, in particolare tramite l'invio automatizzato di *e-mail*, di quanti avevano richiesto preventivi sui servizi resi grazie a un modello (*form*) disponibile sul sito web della società. Nel modello, del quale se ne è prescritta la riformulazione, il potenziale cliente poteva selezionare solo un'unica opzione (mediante apposito box) sia per finalità contrattuali, sia per il trattamento di dati per fini pubblicitari, di ricerche di mercato e sondaggi via *e-mail*. Pur prendendo atto della dichiarazione della società di non aver svolto attività promozionali, il Garante ha ritenuto illecita la raccolta effettuata mediante il *form*. Tra i clienti che non hanno potuto manifestare il libero e specifico consenso per l'invio di comunicazioni automatizzate promozionali, oltre a imprese individuali e liberi professionisti, vi erano anche numerose persone giuridiche, che in base all'art. 130 del Codice, continuano ad essere tutelate riguardo alle comunicazioni promozionali automatizzate (*e-mail*, telefonate, sms). L'Autorità si è riservata di valutare l'applicazione delle sanzioni amministrative previste dal Codice per le violazioni rilevate (provv. 12 gennaio 2017, n. 4, doc. web n. 5986406).

Numerazioni contenute in vecchi elenchi pubblici

In un'altra vicenda, anch'essa oggetto di una segnalazione che evidenziava puntualmente alcune anomalie a partire dal riscontro inizialmente fornito al segnalante dal titolare del trattamento (in effetti rivelatosi, alla luce delle verifiche effettuate, non veritiero), gli accertamenti effettuati *in loco*, anche al fine di acclarare l'origine dei dati del segnalante, hanno, in termini più generali, consentito di appurare che, fino al dicembre 2015, una società aveva utilizzato un *database* interno composto da circa 18.000.000 di numerazioni estratte dagli elenchi telefonici pubblici riferiti all'anno 2007. Rispetto ai dati personali contenuti in tale *database*, in uso a far data dalla costituzione della società e sino a tutto il 2015, non è emerso che esso sia stato mai aggiornato, come invece necessario in base al principio di qualità dei dati (cfr. art. 11, comma 1, lett. *c*), del Codice). Per tale ragione, ancorché alla luce degli elementi acquisiti nel corso degli accertamenti non siano risultate comprovate in concreto operazioni di trattamento per le finalità enunciate nell'art. 7, comma 4, lett. *b*), del Codice, il trattamento di dati così effettuato, relativo ad una banca dati di notevoli dimensioni e prolungato per un ampio arco temporale, compreso tra il 2007 e il 2015, è stato ritenuto illecito, con la conseguenza dell'inutilizzabilità dei dati ai sensi dell'art. 11, comma 2, del Codice, e si è inibito al titolare del trattamento l'ulteriore impiego dei dati presenti nel citato *database* di utenze poiché, per quanto riguarda la possibile effettuazione di "ricerche di mercato", non è risultato acquisito il consenso degli interessati (cfr. il citato provv. 30 marzo 2017, n. 168, doc. web n. 6393365).

***Telemarketing* e prestazioni odontoiatriche**

A seguito del menzionato provvedimento 15 giugno 2017, n. 268 (doc. web n. 6629169) – adottato sulla base di accertamenti propiziati da una dettagliata segnalazione, i cui contenuti sono stati peraltro in larga misura diffusi tramite una trasmissione televisiva di carattere satirico su un'emittente nazionale, oltre che da una segnalazione veicolata dall'Ordine dei medici e odontoiatri della Provincia di Padova – il Garante ha vietato a due società che operano nel settore delle prestazioni odontoiatriche, reputate co-titolari del trattamento, l'ulteriore utilizzo a fini di *telemarketing* di circa un milione di utenze telefoniche fisse e mobili. Dagli accertamen-

ti è risultato che le società hanno trattato in modo illecito i dati acquistati, a quanto consta, da un fornitore di liste stabilito al di fuori del territorio nazionale, senza essere state in grado di dimostrare né l'acquisizione del consenso degli interessati, né l'effettuazione (in quanto rilevante) delle dovute verifiche sul Rpo per appurare l'iscrizione di eventuali utenti che non volessero ricevere telefonate promozionali. Il Garante ha ritenuto altresì incompleta e poco chiara l'informativa fornita agli utenti che si prenotavano *online* e insufficiente il riscontro fornito al segnalante che chiedeva di conoscere la provenienza dei suoi dati e al quale sono state fornite informazioni vaghe e non veritiere. È stato quindi vietato alle società l'uso dei numeri di telefono a fini di *marketing* e si è prescritto loro l'adozione di misure tecniche e organizzative per assicurare agli utenti la piena e tempestiva attuazione dei diritti riconosciuti dal Codice (anzitutto quello avente ad oggetto l'origine dei dati e quello concernente l'opposizione al trattamento).

Le società dovranno inoltre adottare idonee misure tecnologiche per consentire agli utenti del sito di manifestare liberamente il proprio consenso e riformulare il modello di informativa, indicando chiaramente l'ambito di circolazione dei dati e il soggetto cui indirizzare le istanze per l'esercizio dei diritti. Anche in questo caso il Garante si è riservato di contestare, con autonomo procedimento, le sanzioni amministrative per gli illeciti rilevati.

Telemarketing e operatori telefonici

In linea di continuità con le verifiche ispettive condotte dall'Autorità lungo tutto il 2017, nella prima parte del 2018 sono stati adottati provvedimenti, di divieto e prescrittivi, nei confronti dei principali operatori del settore telefonico (cui nella presente Relazione di attività si fa solo cenno) che devono ritenersi particolarmente significativi, vuoi in ragione della dimensione delle violazioni accertate (talora riferite a milioni di contatti commerciali dei quali si è accertata l'effettuazione in violazione di legge: cfr. provv. 8 marzo 2018, n. 140, doc. web n. 8233539; v. pure, nei confronti di altro operatore telefonico, provv. 18 aprile 2018, n. 235, doc. web n. 9358243), vuoi, in particolare in un caso, per la pervasività delle prescrizioni impartite nei confronti del titolare del trattamento finalizzate a ricondurre le operazioni di trattamento per le menzionate finalità commerciali nel rispetto dei diritti degli interessati (cfr. provv. 22 maggio 2018, n. 313, doc. web n. 8995285).

Sotto diverso profilo, nei confronti di altro operatore telefonico già oggetto di provvedimento da parte del Garante per aver effettuato l'attività di *telemarketing* in violazione della disciplina di protezione dei dati (provv. 22 giugno 2016, n. 275, doc. web n. 5255159), è stata adottata dal Garante un'ordinanza ingiunzione di importo rilevante con provvedimento del 18 gennaio 2018, n. 16 (doc. web n. 7665804).

Telemarketing e altri operatori economici

Né in questo ambito si sono arrestati i controlli dell'Autorità: effettuate numerose verifiche nei settori più disparati, sono in corso di valutazione le attività di *telemarketing* effettuate nell'interesse di operatori energetici; sono stati invece adottati alcuni provvedimenti sia nel settore dell'*automotive* (provv. 18 aprile 2018, n. 236, doc. web n. 8983292) come pure nei confronti della commercializzazione di beni di consumo da parte di operatori sedicenti *partner* contrattuali di una multinazionale operante nel settore degli elettrodomestici (provv. 8 febbraio 2018, n. 67, doc. web n. 8187171).

10.4. *Spam* e raccolta di dati personali in internet

Consenso "obbligato" al *marketing* e siti di *e-commerce*

Muovendo dalla segnalazione di alcuni utenti che lamentavano la ricezione di pubblicità indesiderata da parte di una società di *shopping online* e il mancato rispetto del diritto di opposizione al trattamento dei loro dati, l'Ufficio ha effettuato atti-

vità ispettive in collaborazione con il Nucleo speciale *privacy* dalle quali è emerso che gli utenti che desideravano accedere alle sezioni del sito web gestito dalla società di *e-commerce*, ed eventualmente acquistare i prodotti in vetrina, erano prima obbligati a registrarsi e ad accettare (barrando un'apposita casella) le condizioni contrattuali e la *privacy policy* del sito. Con tale adesione l'utente "acconsentiva", con un unico *click*, a che i propri dati venissero utilizzati non solo per le finalità connesse ai servizi offerti *online* (impiego che, ai sensi dell'art. 24, comma 1, lett. *a*), del Codice, non necessita di consenso alcuno da parte dell'interessato), ma anche per le diverse finalità di promozione commerciale, sia da parte della medesima società che da parte dei suoi *partner* commerciali. Una mole ingente di indirizzi *e-mail* e altri dati raccolti in questo modo venivano così registrati in una banca dati per l'invio di pubblicità non richiesta. Muovendo dall'assunto, fondato nella disciplina di protezione dei dati, secondo cui il consenso per il trattamento dei dati personali, per essere valido, non deve essere condizionato, ma libero e specifico, oltre che acquisito prima dell'invio di comunicazioni promozionali, il Garante ha ritenuto illegittimo obbligare una persona al trattamento dei propri dati di contatto per finalità promozionali solo per avere accesso alla "vetrina *online*" di un sito. È stato altresì rilevato che i dati richiesti dalla società in fase di registrazione erano in parte eccedenti oltre che raccolti in violazione dei principi di minimizzazione e di necessità previsti dal Codice, sia in relazione alla sola navigazione nel sito che per l'acquisto dei prodotti ivi commercializzati. Il Garante ha quindi vietato alla società di utilizzare per attività di *marketing* i dati personali raccolti con le descritte modalità (cfr. provv. 20 luglio 2017, n. 324, doc. web n. 6955363).

Social spam

In termini analoghi, il Garante ha ribadito che la presenza di un indirizzo *e-mail* su un *social network* non implica, per ciò solo, che lo stesso possa essere raccolto e destinato all'invio di proposte commerciali, essendo per tale finalità necessario il consenso degli interessati (provv. 21 settembre 2017, n. 378, doc. web n. 7221917). La decisione del Garante ha preso l'avvio dalla segnalazione di una società di consulenza finanziaria che lamentava la ricezione di numerose *e-mail* promozionali da parte dei propri promotori presso i rispettivi indirizzi di posta elettronica senza che ne fosse stato autorizzato l'invio. Dagli accertamenti è emerso che la raccolta di tali indirizzi di posta elettronica era avvenuta con diverse modalità, sia tramite Linkedin e Facebook, sia "pescando" contatti sui *social network*, con l'invio, nell'arco temporale di due anni, di circa 100.000 *e-mail* pubblicitarie. Anche sulla scorta delle linee guida del 4 luglio 2013 – che hanno preso in considerazione il fenomeno del cd. *social spam* –, il Garante ha così ritenuto illecito il trattamento degli indirizzi di posta elettronica acquisiti secondo la menzionata modalità (e, peraltro, in assenza di alcuna informativa resa agli interessati), sull'assunto che l'iscrizione a un *social network* non possa comportare in alcun modo un consenso (neanche implicito) dell'interessato all'utilizzo dei propri dati personali per l'attività di *marketing*. Tale finalità non è compatibile, infatti, con le funzioni dei *social network*, preordinate alla condivisione di informazioni e allo sviluppo di contatti professionali, e non alla commercializzazione di prodotti e servizi. Opinione peraltro sostenuta anche dal Gruppo Art. 29, che ha espressamente escluso che l'iscrizione a un servizio presente sul web comporti la legittimità del trattamento dei dati personali da parte di altri partecipanti alla medesima piattaforma ai fini dell'invio di informazioni commerciali.

Ma si tratta di fattispecie ricorrente: a fronte del persistente invio di *e-mail* promozionali concernenti corsi a pagamento, nonostante l'opposizione dell'interessato, e considerato il mancato riscontro a richieste di informazioni dell'Ufficio, sono stati effettuati accertamenti *in loco* presso una società, nel corso dei quali è emerso che gli indirizzi di posta elettronica dalla stessa utilizzati venivano raccolti, in assen-

za di consenso informato degli interessati, anche in internet, tramite *social network* professionali o attingendo in rete ad elenchi di varia natura (in particolare da ordini professionali ed associazioni). Nel ritenere illecito il trattamento così effettuato (provv. 30 novembre 2017, n. 503, doc. web n. 7522090), con riferimento ai dati personali raccolti dalla società mediante *social network* (nel caso di specie Linkedin), è stato ricordato che anche il Gruppo Art. 29 ha espressamente escluso che il mero accesso ad un sito web, e non diversamente deve ritenersi la mera iscrizione ad un *social network*, per ciò solo comporti la legittimità del trattamento dei dati conferiti da parte di altri partecipanti alla medesima piattaforma ai fini dell'invio di informazioni commerciali. Esemplificando, il Gruppo Art. 29 ha precisato che, nel caso di siti web aventi ad oggetto il gioco *online*, "l'accesso e la partecipazione al gioco non possono essere equiparati alla manifestazione inequivocabile del consenso al trattamento delle informazioni personali per finalità diverse dalla partecipazione al gioco. Il fatto che l'interessato partecipi al gioco non implica che egli intende acconsentire al trattamento dei suoi dati al di là di quanto necessario ai fini del gioco. Questo tipo di comportamento non costituisce una manifestazione inequivocabile della volontà dell'interessato ad accettare l'utilizzo dei suoi dati per finalità commerciali" (cfr. Gruppo Art. 29, WP 187, parere 15/2011 sulla definizione di consenso, adottato il 13 luglio 2011, punto III.A.2, p. 27; cfr. anche il menzionato provv. 11 febbraio 2016; provv. 21 settembre 2017, n. 378, doc. web n. 7221917). Valutazione non diversa è stata estesa anche al trattamento posto in essere dalla società con riguardo ai dati relativi a persone fisiche altre rispetto al segnalante raccolti da elenchi di varia natura disponibili *online*, come nel caso di quelli riferiti ad ordini professionali o ad associazioni di categoria. Anche in tal caso, infatti, deve ritenersi che il trattamento sia stato effettuato in violazione del principio di correttezza e di finalità (art. 11, comma 1, lett. *a*) e *b*), del Codice) e in assenza del consenso preventivo degli interessati richiesto dall'art. 130, commi 1 e 2, del Codice, oltre che in ragione della carenza dell'informativa da rendersi ai sensi dell'art. 13, comma 4, del Codice. Il Garante ha altresì ribadito la necessità del previo consenso informato dell'interessato anche quando i dati personali (come nella fattispecie considerata) siano rinvenibili in internet, in quanto l'agevole reperibilità degli stessi non ne autorizza il trattamento per qualsiasi scopo, ma soltanto per le specifiche finalità sottese alla loro pubblicazione (principio costantemente affermato dal Garante a partire dal provvedimento 11 gennaio 2001, doc. web n. 40823 e, quindi, con il provvedimento generale sullo *spamming* del 29 maggio 2003, doc. web n. 29840 e linee guida *spam*, par. 2.5; provv. 6 ottobre 2016, n. 390, doc. web n. 5834805).

Indirizzi *e-mail* raccolti in internet

Peraltro già in altro provvedimento era stato ritenuto illecito il trattamento di una società per l'invio di comunicazioni promozionali aventi ad oggetto, anche in questo caso, lo svolgimento di corsi di formazione utilizzando in violazione di legge indirizzi *e-mail* raccolti in internet, muovendo da una segnalazione nella quale veniva lamentata la reiterata ricezione di comunicazioni elettroniche a contenuto promozionale nonostante l'assenza del consenso dell'interessato, ed anzi malgrado l'espressa opposizione dallo stesso manifestata ai sensi dell'art. 7, comma 4, lett. *b*), del Codice (peraltro rimasta senza riscontro) (provv. 24 maggio 2017, n. 248, doc. web n. 6502780).

Spam e co-titolarità del trattamento

Sono frequenti i casi in cui vengono segnalati all'Autorità *e-mail* promozionali che, all'esito delle verifiche, sono inviate da soggetti terzi nell'interesse del committente, circostanza risultante nel caso di specie (anzitutto) dal contenuto dei beni pubblicizzati. Entro questa tipologia va ricondotta la fattispecie decisa, a seguito di un reclamo, nel quale pure si lamentava l'impossibilità di bloccare la ricezione di

10

ulteriori messaggi indesiderati mediante gli appositi *link* posti in calce alle *e-mail* (provv. 26 ottobre 2017, n. 437, doc. web n. 7320903). Nel proprio riscontro la società nel cui interesse l'invio delle comunicazioni promozionali era stato effettuato dichiarava di non detenere l'indirizzo di posta elettronica dell'interessato nelle proprie banche dati e di aver affidato l'invio delle *newsletter* ad una società esterna che avrebbe a sua volta subappaltato il servizio ad altra società avente sede in Tunisia. In tale occasione il committente rappresentava altresì che i dati personali del reclamante e il consenso al trattamento degli stessi per finalità di *marketing* sarebbero stati acquisiti all'atto della registrazione in un portale web (circostanza disconosciuta dal reclamante), allegando copia di una *e-mail* nella quale erano indicati data, ora e indirizzo IP relativi alla registrazione dell'indirizzo *e-mail* facente capo asseritamente al reclamante. Nel decidere il reclamo in questione il Garante ha in anteparte reputato il committente co-titolare del trattamento, avendo questi in concreto determinato, secondo quanto stabilito dal Codice (cfr. art. 4, comma 1, lett. *f*), "anche unitamente ad altro titolare" (nel caso di specie il detentore del *database* contenente anche l'indirizzo *e-mail* del reclamante nonché autore dell'invio delle comunicazioni promozionali), "le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati […]". Invio avvenuto, per il tramite della catena di (sub-)contratti, nei quali peraltro alcuna previsione si è rinvenuta in relazione al trattamento dei dati riferiti ai destinatari delle *e-mail* promozionali. In tal senso depone la circostanza secondo cui le decisioni concernenti il trattamento dei dati utilizzati nelle campagne di *marketing* materialmente inviati da altra società, peraltro nel caso di specie stabilita in un Paese terzo, sono state adottate sulla base di una successione di accordi contrattuali "a cascata" attuativi del più ampio accordo stipulato da parte del committente, il quale si poneva come beneficiario delle campagne promozionali effettuate nel proprio interesse e a proprio nome. In tal modo il committente – senza aver posto in essere alcuna preliminare verifica circa il rispetto delle condizioni previste dalla disciplina di protezione dei dati in relazione all'invio delle comunicazioni a contenuto promozionale, né aver in alcun modo disciplinato contrattualmente il ruolo dei *partner* contrattuali chiamati ad effettuare l'invio delle stesse – ha in concreto (co-)determinato le finalità del trattamento: come previsto dal menzionato art. 4, del Codice, esso ha infatti dato impulso all'invio delle comunicazioni a contenuto promozionale (nel caso di specie quelle oggetto del reclamo) e ha altresì individuato modalità e strumenti del trattamento in concreto effettuato (al riguardo v. anche Gruppo Art. 29, WP 169, parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento" adottato il 16 febbraio 2010, p. 8 ss., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_it.pdf). Così operando il committente si è discostato da quanto indicato dal Garante nelle linee guida in materia di attività promozionale e contrasto allo *spam*, nelle quali si è ravvisata "la necessità che i soggetti promotori pongano in essere misure e procedure idonee a conoscere se l'agente, al quale è stato affidato il trattamento dati mediante modalità automatizzate a fini di *marketing*, eventualmente a sua volta si rivolga, per lo svolgimento del medesimo trattamento, a subagenti o altri terzi, nonché a verificare e garantire l'osservanza del Codice da parte di questi ultimi" (p. 3).

Indice ulteriore della ritenuta co-titolarità nel trattamento in questione è stato poi desunto dal contenuto della comunicazione commerciale, inequivocabilmente diretta a promuovere prodotti commercializzati dal committente.

Definito tale profilo, l'illiceità del trattamento è stata dedotta dall'assenza di elementi univoci e sufficientemente circostanziati tali da comprovare il consenso da parte dell'interessato all'utilizzo dei propri dati di contatto per finalità di *marketing*: al riguardo, gli elementi prodotti dal committente (vale a dire l'indirizzo IP regi-

strato in fase di inserimento di raccolta dei dati personali) non sono stati ritenuti sufficienti per affermare univocamente la riconducibilità di detto consenso all'interessato (che peraltro ha espressamente negato la circostanza). Come già rappresentato dal Garante, è infatti necessario che il titolare del trattamento adotti misure idonee a dare prova di tale riconducibilità, fornendo elementi circostanziati tali da poter ritenere acquisito il consenso. In tale prospettiva, nel caso di specie non risulta essere stato adottato alcun sistema di verifica dell'effettiva riconducibilità al reclamante del consenso apparentemente prestato da chi avrebbe effettuato la registrazione dei dati nel menzionato sito web, ad esempio attraverso la modalità, diffusa nella prassi (v. provv. 30 maggio 2013, n. 270, doc. web n. 2603793), dell'invio di una apposita *e-mail* (cd. di conferma) all'indirizzo di posta elettronica utilizzato in fase di registrazione ovvero della conferma della volontà precedentemente manifestata "cliccando" su un apposito *link* (cfr. linee guida in materia di attività promozionale e contrasto allo *spam*, punto 2.6.4; v. già provv. generale in materia di *spam* del 29 maggio 2003, doc. web n. 29840; in tal senso anche Gruppo Art. 29, WP 90, parere 5/2004 relativo alle comunicazioni indesiderate a fini di commercializzazione diretta ai sensi dell'art. 13 della direttiva 2002/58/CE adottato il 27 febbraio 2004, p. 5, secondo il quale "sembra compatibile con la direttiva il metodo consistente nel fatto che un abbonato offra il suo consenso previo registrandosi in un sito web e successivamente sia sollecitato a confermare di essere stato lui la persona che ha effettuato la registrazione"). Misure che, senza comportare onerosi adempimenti (sia in capo al gestore del sito, sia all'interessato), avrebbero potuto assicurare, in ragione della segmentazione della procedura di manifestazione del consenso in due fasi distinte (cd. *double opt-in*), un maggior grado di certezza circa la genuinità della manifestazione del consenso da parte dell'interessato, consentendo così (in prima approssimazione) di prevenire che indirizzi *e-mail* inseriti da terzi o acquisiti *aliunde* all'insaputa e in assenza di autorizzazione alcuna da parte dell'interessato possano essere lecitamente utilizzati (nel caso di specie, per l'invio di comunicazioni promozionali).

Per tali ragioni il Garante ha dichiarato illecito il trattamento dei dati personali consistente nell'invio di messaggi promozionali per posta elettronica effettuato per il tramite di propri *partner* contrattuali nei confronti del reclamante in assenza del consenso dell'interessato ai sensi dell'art. 130, commi 1 e 2, del Codice, prescrivendo altresì al committente l'adozione di idonee misure volte ad assicurare l'utilizzo, per le proprie campagne di *marketing* effettuate anche per il tramite di soggetti esterni, di dati personali relativi ad interessati che abbiano prestato il proprio idoneo consenso.

10.5. *Invio per posta di comunicazioni a contenuto promozionale*

In un reclamo presentato all'Autorità è stato lamentato l'invio di una comunicazione postale a contenuto commerciale contenente un espresso richiamo ad un acquisto effettuato dal destinatario della stessa presso una gioielleria; in base a quanto lamentato, pervenuta detta comunicazione a conoscenza della convivente del segnalante, il contenuto della stessa ingenerava un fraintendimento tale da compromettere il rapporto di coppia. Alla luce degli elementi acquisiti nel corso del procedimento, il Garante ha ritenuto che, ancorché la società non avesse rinvenuto la documentazione relativa al consenso prestato dal reclamante all'invio di comunicazioni commerciali, tale consenso fosse stato effettivamente prestato (come peraltro dichiarato dal reclamante, che aveva riconosciuto di aver "fornito un'autorizzazione

10

a ricevere materiale promozionale generico", e come risultante dai sistemi informativi della società). Anche analizzando il modello di informativa fornita alla clientela, dalla stessa era possibile desumere l'impiego dei dati del cliente "per fornire servizi personalizzati di vendita presso i negozi […] di tutto il mondo". Tale finalità, espressa in termini generali, trovava poi esemplificazione (sia nell'informativa che nel modello predisposto per la manifestazione del consenso) nelle modalità attraverso le quali detti servizi avrebbero potuto essere resi (anche in forma di invio di comunicazioni promozionali, pure personalizzate, come nel caso di specie). Per tali ragioni il Garante non ha ritenuto illecito il trattamento effettuato dalla società, prescrivendo tuttavia nei confronti di quest'ultima di dotarsi di adeguate procedure interne aventi ad oggetto le modalità di conservazione dei supporti materiali contenenti i dati personali della clientela, impartendo le necessarie istruzioni relative alla corretta conservazione degli stessi ai propri responsabili ed incaricati del trattamento (provv. 13 settembre 2017, n. 370, doc. web n. 7297817).

11 Internet e servizi di comunicazione elettronica

11.1. *Diffusione di dati personali in internet*

Divulgazione di dati riferiti a minore su un *social network*

Con provvedimento 23 febbraio 2017, n. 75 (doc. web n. 6163649) il Garante ha prescritto ad una madre di rimuovere dalla propria pagina Facebook due provvedimenti giurisdizionali, concernenti la cessazione degli effetti civili del matrimonio, in cui erano riportati delicati aspetti di vita familiare che riguardavano anche la figlia minorenne. Il Garante – intervenuto su segnalazione dell'ex marito che lamentava una violazione del diritto alla riservatezza della figlia – ha ritenuto che la divulgazione dei provvedimenti giurisdizionali in questione fosse incompatibile con quanto stabilito dal Codice che vieta la pubblicazione "con qualsiasi mezzo" di notizie che consentano l'identificazione di un minore coinvolto in procedimenti giudiziari, nonché la diffusione di informazioni che possano rendere identificabili, anche indirettamente, i minori coinvolti e le parti in procedimenti in materia di famiglia. Secondo il Garante, inoltre, l'estrema pervasività della divulgazione su internet aggrava notevolmente la violazione di diritti della persona, in questo caso per giunta minore di età. Non può essere provata, infatti, la persistente natura "chiusa" del profilo e la sua accessibilità a un gruppo ristretto di "amici", perché il profilo è facilmente modificabile, da "chiuso" ad "aperto", in ogni momento da parte dell'utente. Vi è inoltre la possibilità che un "amico" condivida il cd. *post* con le sentenze sulla propria pagina, rendendolo visibile ad altri iscritti, determinando così una possibile conoscibilità "dinamica", più o meno ampia, del contenuto che può estendersi potenzialmente a tutti gli iscritti a Facebook.

Nel disporre la rimozione, il Garante ha altresì sottolineato che le sentenze consentono di rendere identificabile la bambina nella cerchia di persone che condividono le informazioni "postate" dalla madre sul proprio profilo e contengono riferimenti molto delicati, anche inerenti alla sfera sessuale, al vissuto familiare e a disagi personali della minore.

Diffusione di dati in internet

Al di là delle ipotesi di violazione dei dati ai sensi dell'art. 32-*bis* del Codice (cfr. par. 11.3), merita qui menzionare altri casi che, pur non rientrando in tale ambito (a legislazione vigente), comunque hanno comportato la diffusione di dati personali in internet, rispetto ai quali l'Autorità, a seguito di segnalazione, è tempestivamente intervenuta con provvedimenti di blocco adottati, per ragioni di urgenza, dal Presidente del Garante. In un primo caso è stato accertato che, accedendo all'area del sito riservata alla clientela di una società erogatrice di servizi idrici, risultavano liberamente consultabili una serie di *link* a *file* e cartelle contenenti dati personali, del segnalante e di altri soggetti, concernenti operazioni di pagamento effettuate *online*. Risultavano facilmente reperibili nominativi, indirizzi e persino numeri di carte di credito – anche se parzialmente oscurati – oltre alla data di scadenza delle stesse. Il Garante ha ritenuto illecita tale pubblicazione di dati che, per tipologia e numerosità, esponeva gli interessati al rischio di pregiudizi rilevanti, tra cui quello di furto d'identità, con conseguente provvedimento di blocco della diffusione dei dati (cui il titolare del trattamento ha comunicato di essersi conformato) (provv. 31 gennaio 2017, n. 3, doc. web n. 6026547).

Analogamente, è stato disposto il blocco dell'ulteriore diffusione in internet di n. 290 *file*, contenenti scansioni di documenti riconducibili a diverse centinaia di interessati, suscettibili di essere liberamente consultati e acquisiti da chiunque perché non protetti da alcuna procedura di autenticazione (provv. 12 dicembre 2017, n. 527, doc. web n. 8761841).

Attivazione di servizi di comunicazione elettronica non richiesti

A fronte dell'indebita attivazione di un servizio di comunicazione elettronica (opzionale) non richiesto sull'utenza residenziale del segnalante – in base a quanto rappresentato dal titolare del trattamento dovuta a un possibile fraintendimento sulla base del quale è stato emesso l'ordine di attivazione dall'operatore del *customer care*, nell'ambito di uno scambio di informazioni di natura amministrativa e considerata la documentazione complessivamente acquisita, dalla quale non risultava comprovato che il segnalante abbia in alcun modo prestato il proprio consenso per l'attivazione del servizio –, il Garante ha ritenuto illecito il conseguente trattamento di dati personali riferito all'interessato in associazione all'attivazione del servizio opzionale, in quanto effettuato in violazione del principio di correttezza di cui all'art. 11, comma 1, lett. *a*), del Codice nonché in assenza di uno dei presupposti di cui agli artt. 23 e 24 del Codice, con la conseguente adozione del provvedimento 26 ottobre 2017, n. 439 (doc. web n. 7339171).

11.2. *Ricerche inverse*

Sync.me

A fronte di alcune segnalazioni concernenti il trattamento di dati personali effettuato mediante il sito Sync.me e l'omonima app – un'applicazione per *smartphone* preordinata all'identificazione di un chiamante sconosciuto, al blocco delle chiamate o dei messaggi indesiderati in entrata, a creare una lista di numeri indesiderati, a mantenere aggiornate le informazioni dei propri contatti (data di nascita, genere, indirizzo fisico, foto o indirizzi *e-mail*) mediante sincronizzazione con i principali *social network* (Facebook, Google+, Twitter, Linkedin) e a costituire un elenco telefonico consentendo altresì la ricerca inversa a partire dai numeri –, nelle quali si lamenta una possibile violazione delle discipline di protezione dei dati personali, con particolare riferimento all'utilizzo dei dati di terzi raccolti mediante la rubrica di chi utilizza l'applicazione in questione, all'insaputa ed in assenza del consenso degli interessati, l'Autorità ha effettuato primi approfondimenti, anche in cooperazione con altre autorità di controllo europee.

11.3. Data breach

***Data breach* nei sistemi di gestione della clientela**

È stata portata all'attenzione dell'Autorità l'ingiustificata attivazione, a nome del reclamante e a sua insaputa, di un numero elevato di linee di telefonia residenziale (oltre 800) da parte di una società di telecomunicazioni; dell'accaduto il reclamante sarebbe venuto a conoscenza, a far data dal dicembre 2011, in occasione del verificarsi di alcune attività di recupero crediti (via via infittitesi), effettuate con solleciti telefonici e scritti indirizzati a sé e alla moglie e provenienti da operatori a ciò incaricati dalla società. Di qui, ritenuti insoddisfacenti i riscontri della società ai numerosi reclami alla stessa presentati e alle istanze di accesso ai sensi dell'art. 7 del Codice – finalizzate ad accertare, tra l'altro, l'esatto numero di linee a sé associate –, nel reclamo presentato al Garante è stato lamentato il trattamento illecito dei dati relativi al reclamante, per un ampio lasso temporale, compreso tra il 2003 e il 2015, e nonostante la società fosse a conoscenza di tale circostanza; trattamento di dati che

non si sarebbe esaurito nell'indebita attribuzione al reclamante di linee telefoniche allo stesso estranee, ma che avrebbe trovato ulteriore sviluppo nell'indebita comunicazione di dati personali a terzi (anzitutto ad una pluralità di operatori di recupero del credito, ausiliari della società oltre che ai destinatari di fatture dalla stessa trasmesse recanti l'indebito inserimento del proprio codice fiscale).

Considerati gli elementi contenuti nel reclamo, al fine di verificare le circostanze rappresentate nonché, più in generale, l'osservanza delle disposizioni in materia di protezione dei dati personali da parte della società, l'Ufficio ha completato nel 2017 le verifiche *in loco* presso alcune sedi della società iniziate a fine 2016. All'esito di tali verifiche (che hanno riguardato anche altri clienti individuati a campione in occasione degli accessi ai sistemi informativi della società) è stato possibile appurare (cfr. provv. 6 aprile 2017, n. 176, doc. web n. 6376175), che le numerose assegnazioni di linee telefoniche registrate in passato in capo al reclamante (e risultate dall'esame dei sistemi della società) non trovavano fondamento in alcun contratto intercorso tra le parti (né sono risultate frutto di condotte abusive da parte di terzi). L'erronea attribuzione delle linee telefoniche (in quanto disancorata rispetto ai contratti intercorsi con gli effettivi contraenti) sarebbe dovuta a (non meglio precisati) errori occorsi durante le attività di migrazione massiva di dati della clientela dal sistema gestionale preesistente a quello in uso e ha interessato, per un lungo arco temporale, un novero di soggetti più ampio (non precisamente delimitabile al tempo delle verifiche e in sede di adozione del successivo provvedimento) rispetto al solo reclamante.

Alla luce delle circostanze di fatto accertate, è stato quindi ritenuto illecito il trattamento di dati personali consistente nell'associazione, anzitutto in capo al reclamante (ma che ha interessato, come detto, una più ampia platea di soggetti), di utenze residenziali e la comunicazione a terzi di dati personali che lo riguardano sulla base dell'erronea assegnazione delle utenze. Al riguardo il Garante ha ritenuto effettuate in violazione dei principi di qualità dei dati (cui all'art. 11, comma 1, lett. *b*), del Codice) nonché in assenza di alcuna base giuridica (ai sensi degli artt. 23 e 24 del Codice) le operazioni di trattamento che hanno determinato l'attribuzione, in capo al reclamante, di un numero rilevante di utenze telefoniche residenziali nel sistema gestionale (e la loro persistenza, nonostante i reclami pervenuti alla società), con la conseguente propagazione di tali informazioni su altri sistemi (tra i quali, quello di fatturazione e quello preordinato a consentire la corretta effettuazione di verifiche da parte delle Forze di polizia e della magistratura) nonché l'attribuzione in capo allo stesso della qualità di "moroso", nella misura in cui la stessa fosse riconducibile al mancato pagamento di fatture relative a linee telefoniche delle quali non è stato reale intestatario.

Il Garante ha altresì stigmatizzato la condotta negligente e omissiva tenuta dalla società la quale, per un periodo prolungato, anche in tempi successivi alla segnalazione dell'erroneità delle predette assegnazioni, in violazione del principio di correttezza nel trattamento (art. 11, comma 1, lett. *a*), del Codice), non ha svolto le necessarie verifiche che avrebbero potuto assicurare l'approntamento di rimedi nei confronti del reclamante anzitutto e, quindi, di quanti si trovavano in una situazione analoga.

Né si è ritenuto che venisse meno l'illiceità della condotta tenuta sulla base degli asseriti malfunzionamenti dei propri sistemi informativi nella fase di "travaso" dei dati dal vecchio sistema gestionale al nuovo, della cui eziologia il titolare del trattamento non è stato in grado di fornire prova alcuna. Al contrario, la difficoltà nel far luce sulla natura e sulle ragioni dei malfunzionamenti verificatisi, oltre che di porre rimedi agli stessi con adeguate misure tecniche che non si limitassero a "tamponare" la singola richiesta, ma ad incidere strutturalmente sull'architettura informativa del

sistema gestionale, lungi dall'allontanare la riconducibilità alla società di quanto avvenuto, e quindi la sua responsabilità a tale riguardo (cfr. art. 15 del Codice), evidenzia una poco attenta gestione dei menzionati sistemi che rappresentano i gangli vitali della propria infrastruttura informativa, interessando direttamente la clientela. Inoltre, tale responsabilità non è venuta meno, ed anzi si è aggravata, con l'inerzia tenuta dalla società dopo che, pur avendo avuto, in più occasioni, notizia dell'accaduto dal reclamante nonché da altri clienti, anche in relazione all'erroneo inserimento in fattura di un dato quale il codice fiscale, non ha dato prova – secondo gli standard di diligenza richiesti per un operatore economico di rilevanza primaria nel settore delle comunicazioni elettroniche – di aver posto in essere alcuna idonea misura per definire il perimetro dei malfunzionamenti ed eliminarne le conseguenze pregiudizievoli in capo al reclamante, anzitutto, ma anche, come si è visto, in capo agli altri clienti interessati da quanto verificatosi.

Il Garante ha anche criticamente evidenziato le modalità di esecuzione delle cd. bonifiche effettuate nel corso del tempo, realizzate in modo puntiforme, senza l'effettuazione di alcuna valutazione circa la più ampia portata delle segnalate anomalie che avrebbero dovuto essere considerate, dato il significato dell'informazione relativa al codice fiscale dei clienti nei sistemi gestionali della società, "eventi sentinella" rispetto al più ampio fenomeno dei disallineamenti oggetto di accertamento. "Bonifiche" peraltro eseguite senza predisporre idonea documentazione volta a rappresentare compiutamente le operazioni poste in essere, sì da tenere traccia dell'andamento storico dei fatti; inoltre, con riguardo al sistema funzionale a dare riscontro alle richieste provenienti dalla magistratura e dalla Forze di polizia, è stata censurata l'impossibilità di comprendere, dalla consultazione dello stesso, l'erroneità nell'assegnazione in capo al reclamante (e, più in generale, ai clienti impropriamente qualificati come assegnatari) delle linee contestate.

Ulteriore profilo di censura ha riguardato le modalità, ritenute non corrette, di attuazione, in primo luogo nei confronti del Garante, di quanto previsto dall'art. 32-*bis* del Codice: ciò, sia in relazione alla (in)tempestività della comunicazione della violazione dei dati, rispetto a disallineamenti già noti alla società, sia in relazione al contenuto delle informazioni indicate nella comunicazione diretta all'Autorità, attesa la significatività dell'erroneo inserimento del codice fiscale nelle fatture e dello spettro di conseguenze connesse a tale circostanza o delle quali tale circostanza avrebbe dovuto essere rivelatrice (elementi che avrebbero dovuto essere esplicitati nella comunicazione della società), sia in relazione alle possibili ripercussioni negative cui il reclamante (e gli altri interessati) avrebbero potuto andare incontro. Il Garante ha altresì censurato, alla luce degli elementi emersi negli accertamenti, da un lato, l'erroneità dell'indicazione di un solo individuo (il reclamante) come soggetto interessato dall'evento, atteso che, mediante l'esecuzione di ordinarie verifiche, si sarebbe rilevata, come accaduto nel corso degli accertamenti, l'esistenza di una ben più ampia (peraltro indefinita) rosa di soggetti interessati dall'evento occorso; dall'altro, il livello sottostimato, in ragione di quanto precede, della gravità della violazione dei dati personali occorso, valutato dalla società in "basso/trascurabile". Per tali ragioni si è ritenuto che la società non abbia dato tempestivo ed integrale adempimento a quanto prescritto dall'art. 32-*bis*, comma 2, del Codice (oltre che rispetto all'obbligo di riscontro integrale alle richieste fatte valere in sede di esercizio del diritto di accesso ex art. 7 del Codice) nei confronti dell'interessato, al quale non sono state correttamente rappresentate (in violazione peraltro del principio di correttezza nel trattamento di cui all'art. 11, comma 1, lett. *a*), del Codice) le conseguenze dell'evento e il numero complessivo delle utenze telefoniche allo stesso erroneamente associate nei sistemi della società (pari a 826), ma un numero significativamente più ridotto (pari a 42).

Alla luce di tali complessive considerazioni, al di là dell'accertamento dell'illiceità dei trattamenti effettuati (ivi compresa l'indebita comunicazione a terzi di dati rivelatisi inesatti) e della mancata adozione di misure di sicurezza idonee ad assicurare l'integrità, l'esattezza e l'aggiornamento dei dati trattati, con conseguente violazione dell'art. 32, comma 1, del Codice, al titolare del trattamento sono state impartite puntuali e articolate prescrizioni – peraltro oggetto di differimento in ragione della numerosità dei sistemi interessati dalle verifiche e della entità delle misure da adottare (provv. 26 luglio 2017, n. 344, doc. web n. 6821640) – concernenti sia la persona del reclamante, sia la posizione di altri clienti (attivi e cessati) interessati da analoghi disallineamenti. Tali prescrizioni si sono incentrate sulla previa verifica e sulla successiva attività di "bonifica" (secondo le modalità indicate nel provvedimento) in tutti i sistemi della società, dell'esattezza dei dati personali riferiti o associati al reclamante (e rispetto a quanti, in presenza di una discordanza tra i dati riferiti all'intestatario della linea telefonica e l'intestatario della fattura, venissero a trovarsi in condizioni analoghe), con la conseguente annotazione negli stessi che ciascuna delle linee erroneamente attribuite, ancorché cessate, non avesse mai fatto capo agli stessi (e la contestuale annotazione dell'intestatario effettivo), nonché sull'eliminazione della qualifica di "moroso" indebitamente attribuita a quanti interessati dai rilevati disallineamenti. Al fine di facilitare i controlli rispetto alla platea dei soggetti (potenzialmente) interessati dai disallineamenti, è stato indicato alla società, in occasione dell'invio di comunicazioni alla clientela (quali, ad es., le fatture in scadenza), di inserire nelle stesse, in posizione e con modalità grafiche che ne assicurassero immediata visibilità, un apposito invito rivolto al destinatario della comunicazione a verificare la correttezza dei dati di fatturazione, con particolare riferimento al codice fiscale e all'eventuale indirizzo di posta elettronica ivi presenti, con l'indicazione di un recapito, se del caso dedicato, cui segnalare le rilevate incongruenze.

È stato inoltre prescritto alla società, con riguardo al profilo della avvenuta (illecita) comunicazione dei dati, di effettuare una ricognizione volta ad accertare a quali soggetti i dati di quanti interessati dell'erronea assegnazione delle linee telefoniche fossero stati trasmessi per quindi comunicare ad essi, con cadenza mensile rispetto ai soggetti via via individuati, l'erronea assegnazione delle linee con la contestuale indicazione del reale intestatario delle stesse al fine di consentire le necessarie rettifiche.

È stato infine prescritto alla società, al fine di minimizzare il rischio rispetto ai dati personali trattati per finalità di recupero del credito relativi a soggetti non effettivi intestatari di linee, di adottare idonee misure organizzative, affinché, in caso di discordanza tra l'intestatario della linea e l'intestatario della fattura, anteriormente ad ogni azione di recupero del credito, anche mediante ausiliari della società, venissero effettuate preventive verifiche volte a scongiurare che soggetti che non rivestono la qualifica di debitore siano ingiustificatamente contattati; è stato anche prescritto che tutto il personale del *customer care*, in caso di rilevata discordanza tra i dati riferiti all'intestatario della linea e all'intestatario della fattura, anche a seguito di reclamo da parte della clientela, segnali tempestivamente le anomalie alle funzioni interne cui è rimesso il compito di effettuare le "bonifiche".

Dal punto di vista sanzionatorio, in ragione della rilevata illiceità dei trattamenti connessi alla violazione dei dati, il Garante ha adottato ordinanza ingiunzione con provvedimento del 16 maggio 2018, n. 297 (doc. web n. 9370122).

Nel conformarsi alle prescrizioni contenute nel provvedimento, la società ha provveduto a comunicare all'Autorità, con periodicità, nel corso del 2017 e dei 2018, lo stato di attuazione delle stesse.

Anche da parte di altro primario operatore di servizi di comunicazione elettronica è stata comunicata all'Autorità, ai sensi dell'art. 32-*bis* del Codice, l'avvenuta vio-

***Data breach* nell'area clienti**

lazione di dati personali con riguardo al proprio sistema informatico di *self care*, con la conseguente visualizzazione di credenziali contenute in un *file* recante dati personali riferiti a 5.118 clienti (di cui 683 non più attivi), per una parte dei quali, informati dalla società che pure ha inibito l'accesso al sistema ed avviato la procedura di cambio *password*, poteva anche essersi verificato un accesso non autorizzato all'area personale nell'area clienti. Circostanza quest'ultima che avrebbe consentito la visualizzazione di alcuni dati personali della clientela (nominativo, codice fiscale, recapito telefonico *e-mail*, indirizzo di residenza e, solo per i clienti che ne hanno fatto richiesta, fatture degli ultimi sei mesi con il dettaglio del traffico in uscita parzialmente oscurato) e l'effettuazione di alcune modifiche.

Alla luce delle verifiche *in loco* condotte dall'Ufficio, è stato possibile dapprima acclarare che il *file* di testo oggetto di violazione è stato generato nel corso di un intervento sistemistico, eseguito dal fornitore di servizi e conclusosi a settembre 2016, volto a migliorare le *performance* (cd. *tuning*) dei sistemi di tracciatura degli accessi alla applicazione *self care* esposta sul portale della società e, per cause legate ad un'errata impostazione delle regole di denominazione dei *file* (cd. *naming*) generati dal sistema di tracciatura, non è stato automaticamente cancellato al termine dell'intervento. Rilevato che la società, a fronte di una violazione che, in base a quanto dichiarato, ha interessato 5.118 utenti, ha provveduto ad informare solo i 402 clienti per i quali è risultato un accesso all'area personale nelle ore in cui l'incidente era in corso ritenendo, anche in considerazione delle misure correttive approntate (tra cui il blocco degli accessi al portale ed il *reset* delle *password*), che solo per essi potesse configurarsi un potenziale pregiudizio coincidente con l'accesso alle numerose informazioni contenute nell'area clienti, il Garante ha tuttavia ritenuto che già la sola acquisizione di credenziali di accesso sia da ritenere di per sé fonte di potenziale pregiudizio per gli interessati, indipendentemente dal fatto che ne consegua un effettivo utilizzo per accedere a specifiche aree riservate, in considerazione della probabilità che le medesime credenziali possano essere utilizzate per accedere a diversi portali web (atteso che la *user-id* è costituita dal numero telefonico dell'utente). Al riguardo, il Garante ha già chiarito nel provvedimento del 4 aprile 2013 (cfr. punto 7, ultimo cpv.) che "devono essere sempre comunicate immediatamente ai contraenti le violazioni che riguardano le credenziali di autenticazione (nome utente e *password*, ancorché quest'ultima sia cifrata)". Nel caso di specie, peraltro, la società ha dichiarato in sede di accertamento ispettivo che le credenziali di autenticazione presenti nel *file* violato erano riportate in chiaro e che la *user-id*, costituendo un dato di per sé direttamente e univocamente identificativo, alla luce delle tecnologie disponibili, può essere utilizzata come chiave per individuare in rete l'utente e conseguentemente accedere anche ad altre informazioni allo stesso correlate. Dovendo, ai fini della comunicazione agli interessati, essere prese in considerazione, tra le altre, le probabili conseguenze della violazione di dati personali per l'interessato, in particolare nel caso in cui "la violazione possa comportare furto o usurpazione di identità" (art. 3, par. 2, lett. *b*), del regolamento (UE) n. 611/2013) nonché "le circostanze della violazione di dati personali, in particolare nel caso in cui i dati siano stati rubati" (art. 3, par. 2, lett. *c*), del regolamento (UE) n. 611/2013), il Garante ha prescritto alla società, di informare con comunicazione scritta e senza ritardo, anche gli interessati non già destinatari della precedente comunicazione dell'avvenuta violazione dei dati (provv. 11 maggio 2017, n. 226, doc. web n. 6431926).

A seguito dell'esame della documentazione relativa a tale violazione dei dati (in tempi successivi all'adozione del provvedimento testè mensionato), è stata rilevata la presenza di un numero più elevato di soggetti interessati dalla violazione dei dati

rispetto a quanti indicati nell'originaria notifica al Garante e pure le informazioni oggetto di violazione sono risultate più articolate per tipologia rispetto a quanto notificato. Dai successivi approfondimenti è risultato infatti che la violazione ha riguardato non solo numeri di utenze telefoniche e *password* per l'accesso all'area *self care* ma anche numeri di utenza telefonica, talora associati all'indirizzo *e-mail* degli interessati o alla "domanda segreta" scelta per effettuare la modifica delle *password* o, ancora, sporadicamente, abbinati a numeri di carta payback o a dati bancari. Tali elementi sono stati arricchiti dagli esiti di ulteriori accertamenti effettuati presso la società, nel corso dei quali è risultato confermato un numero più elevato di soggetti coinvolti dalla violazione, pari a circa 28.000 clienti.

Alla luce di tali (ulteriori) risultanze e considerato che l'accesso non autorizzato è avvenuto in conseguenza di un attacco informatico finalizzato alla ricerca e all'acquisizione di dati personali, il Garante ha prescritto alla società di informare dell'avvenuta violazione dei dati, senza ritardo e con le modalità semplificate ritenute più opportune, anche quanti (su iniziativa della società o in base al menzionato provvedimento n. 226 del 2017) non ne erano già stati informati (provv. 26 luglio 2017, n. 343, doc. web n. 6821202).

11.4. *Dati di traffico*

In ragione del fatto che, alla data del 1° luglio 2017, le disposizioni di cui all'art. 4-*bis*, d.l. 18 febbraio 2015, n. 7 (convertito con modificazioni dalla l. 17 aprile 2015, n. 43, come modificato dal d.l. 30 dicembre 2015, n. 210, convertito con modificazioni dalla l. 25 febbraio 2016, n. 21), recante disposizioni in materia di conservazione dei dati di traffico telefonico e telematico, non trovavano più applicazione con riguardo alla proroga dei termini per la conservazione dei dati di traffico, in deroga a quanto stabilito dall'art. 132, comma 1, del Codice, l'Ufficio ha invitato cinque tra i principali operatori di comunicazioni elettronica a far conoscere all'Autorità le misure adottate. Nei riscontri forniti, tutti gli operatori hanno confermato di avere posto in essere le procedure di cancellazione dei dati di traffico, limitandone la conservazione solo per le finalità di cui all'art. 132 del Codice.

Come anticipato (v. par. 2.1.1), nella materia in parola è tuttavia nuovamente intervenuto il legislatore, con la l. 22 novembre 2017, n. 167 (Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017), che, all'art. 24, con riguardo ai termini di conservazione dei dati di traffico telefonico e telematico dispone: "In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficaci in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-*quater*, e 407, comma 2, lettera *a*), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-*bis*, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-*bis*, del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196". Rilevata la sproporzione di tali tempi di conservazione, il Garante, con nota del Presidente 22 dicembre

11

2017 (doc. web n. 7464029), ha segnalato tale valutazione a Governo e Parlamento, ponendo in rilievo la contrarietà della disposizione di recente adozione con l'ordinamento eurounitario e la giurisprudenza della CGUE (cfr. sentenza 8 aprile 2014 (*Digital rights Ireland*); CGUE, Grande Camera, con sentenza 21 dicembre 2016 (cause riunite C-203/15 e C-698/15), auspicandone un ripensamento in occasione dell'attuazione del nuovo quadro comunitario in materia di protezione dei dati personali.

12 Il trattamento dei dati personali da parte di movimenti politici

Piattaforma Rousseau

Con provvedimento 21 dicembre 2017, n. 548 (doc. web n. 7400401) è stata definita l'istruttoria avviata ad agosto 2017, allorquando si è avuta notizia di una intrusione informatica ai danni della cd. piattaforma Rousseau e del *blog* www.beppegrillo.it, con conseguente violazione dei dati personali di numerosi interessati. In particolare, a seguito di un intervento ispettivo presso la sede dell'Associazione Rousseau (che, con una sola eccezione rispetto ai diversi siti riconducibili al Movimento 5 Stelle, è risultata essere stata designata responsabile del trattamento), il Garante ha prescritto l'adozione di alcune misure necessarie (e altre opportune) da adottare entro il termine di 30 e 60 giorni dalla ricezione del provvedimento al fine di assicurare la piena legittimità del trattamento dei dati degli iscritti e dei militanti del Movimento 5 Stelle e garantire la sicurezza informatica dei sistemi utilizzati. Si tratta, da un lato, di indicazioni relative alle informative e al consenso, fino alla necessaria designazione di alcuni soggetti quali responsabili del trattamento; dall'altro, di misure concernenti il miglioramento della resistenza alla vulnerabilità della piattaforma e degli strumenti connessi, l'adeguamento dei sistemi di autenticazione, il ricorso ai protocolli "https", l'impiego di algoritmi crittografici nella conservazione delle basi dati e l'attuazione di *auditing* informatici per assicurare la sicurezza dei dati.

Alcune perplessità sono state sollevate dall'Autorità in ordine alle misure di sicurezza connesse alle operazioni di voto svolte all'interno del Movimento; in particolare, ferma restando la libertà di ogni associazione privata – qual è un movimento o partito politico –, si è ritenuto che il sistema di *e-voting* debba essere riconfigurato in modo da minimizzare i rischi per i diritti e per le libertà delle persone, in accordo al principio di *data protection by default* e, in prospettiva, alle previsioni di cui all'art. 32, par. 1, lett. *a*), RGPD, prevedendo la cancellazione o la trasformazione in forma anonima dei dati personali trattati al termine delle operazioni di voto.

Propaganda via sms

L'Autorità ha altresì esaminato alcune segnalazioni nelle quali veniva per lo più lamentato il reiterato invio di sms di natura politica e propagandistica da parte del PD nazionale e del PD Roma, non di rado nonostante il previo esercizio dei diritti di cui all'art. 7 del Codice (e in particolare di quello di cancellazione dei dati e opposizione al trattamento) nei confronti della formazione politica che non ha dato seguito agli stessi. All'esito dell'istruttoria sono stati accertati l'insoddisfacente riscontro (dal punto di vista della tempestività e dell'esaustività) nei confronti delle istanze formulate dai segnalanti ai sensi dell'art. 7 del Codice nonché profili di illiceità dei trattamenti effettuati in violazione dell'opposizione manifestata dagli interessati, profili per i quali l'Autorità si è riservata di avviare il relativo procedimento sanzionatorio (note 25 gennaio 2018).

Propaganda via *e-mail*

Non diversamente, è stato ritenuto in violazione di legge l'invio di *e-mail* a contenuto propagandistico avvenuto ad opera di un ex assessore del Comune di Napoli: l'uso in concreto dell'indirizzo di posta elettronica della segnalante per finalità propagandistiche, risultato acquisito nell'ambito dell'esercizio delle funzioni istituzionali, non è stato ritenuto conforme ai principi di correttezza e finalità (art. 11, comma 1, lett. *a*) e *b*), del Codice). In particolare, l'originaria raccolta dei dati riferiti alla segnalante da parte dell'amministrazione comunale era finalizzata a consen-

12

tire eventuali contatti con la stessa per l'assolvimento delle funzioni istituzionali, finalità questa non compatibile con quella del loro utilizzo, diverso e ulteriore, per finalità di natura propagandistica (nel caso in esame, una volta cessato l'incarico assessorile). Ciò in linea con quanto costantemente affermato dal Garante con riguardo ai dati raccolti o utilizzati per lo svolgimento di attività istituzionali (cfr. provv. 6 marzo 2014, n. 107, par. 5.4.1. lett. A; v. pure provv. 5 maggio 2016, n. 205, doc. web n. 6358149), secondo cui, nel rispetto del principio di compatibilità di cui all'art. 11, comma 1, lett. *b*), del Codice, le fonti documentali detenute dai soggetti pubblici non sono utilizzabili a scopo di propaganda elettorale e connessa comunicazione politica in ragione della specifica disciplina di settore che ne preclude l'acquisizione per il perseguimento dei predetti fini e ciò anche in relazione ai dati raccolti dai soggetti pubblici nello svolgimento delle proprie attività istituzionali o, in generale, per la prestazione di servizi (nota 25 gennaio 2018).

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

13.1. *Protezione dei dati personali e rapporto di lavoro*

Una volta completata ed applicata a pieno regime la riforma del mercato del lavoro (cd. *Jobs Act*) con i decreti legislativi di attuazione della legge delega n. 183/2014, alcuni dei quali hanno avuto importanti riflessi sulla normativa in materia di protezione dei dati personali (d.lgs. nn. 150/2015 e 151/2015), anche nel 2017 sono stati portati all'attenzione dell'Autorità diversi casi di trattamenti di dati effettuati nell'ambito del rapporto di lavoro rispetto ai quali ha trovato applicazione la nuova disciplina dei controlli a distanza della prestazione lavorativa (art. 4, l. n. 300/1970, come modificato dall'art. 23, d.lgs. n. 151 cit.).

In tali occasioni il Garante ha avuto modo di affrontare alcuni aspetti meritevoli di attenzione sul piano interpretativo ed applicativo, approfondendo l'impatto della predetta disciplina lavoristica sulle garanzie e sui diritti previsti dalla normativa in materia di protezione dei dati personali, al fine di individuare il corretto bilanciamento fra i diversi interessi in campo.

Già nel 2016 l'Autorità, in un provvedimento adottato nei confronti di un ateneo, aveva espresso il proprio orientamento sull'ambito di applicazione del comma 2 del predetto art. 4 dello Statuto dei lavoratori mediante una possibile "perimetrazione" degli "strumenti utilizzati dal lavoratore per rendere la "prestazione lavorativa", in presenza dei quali vengono meno talune garanzie per gli interessati sul piano lavoristico (provv. 13 luglio 2016, n. 303, doc. web n. 5408460; cfr. Relazione 2016, p. 100). In questo ambito – e, più in generale, sul rapporto fra disciplina lavoristica in materia di controlli a distanza e garanzie poste a protezione dei dati personali dei lavoratori – il Garante è intervenuto anche nel periodo di riferimento, tenendo conto della specificità dei trattamenti e degli strumenti utilizzati in concreto dal datore di lavoro dai quali è risultato "indirettamente" il controllo dell'attività lavorativa.

Ciò è avvenuto prevalentemente rispetto a trattamenti di dati personali effettuati attraverso sistemi che consentono la localizzazione geografica dei dipendenti; l'installazione di dispositivi tecnologici dotati di tale funzionalità (ormai agevolmente reperibili sul mercato, a costi contenuti, pure attraverso la fornitura dei relativi servizi da parte di società specializzate) ha costituito infatti l'oggetto di una quota significativa dell'attività dell'Autorità in materia di trattamenti in ambito lavorativo, sia in sede di decisione di istanze di verifica preliminare sia con riferimento alla definizione di casi oggetto di reclami e/o segnalazioni nonché all'esito di accertamenti ispettivi disposti anche d'ufficio.

Il Garante è altresì intervenuto in merito al trattamento di dati biometrici dei lavoratori (cfr. par. 13.5), come pure in tema di videosorveglianza (cfr. par. 13.4).

Non sono mancate infine altre pronunce sul trattamento di dati personali nella gestione del rapporto di lavoro, con particolare riguardo al trattamento di dati giudiziari (cfr. par. 13.6) o di dati sanitari (cfr. par. 13.7).

13.2. *Il trattamento dei dati relativi ai dipendenti tramite sistemi di geolocalizzazione*

Nel corso dell'anno di riferimento il Garante ha valutato le finalità e le concrete modalità di funzionamento dei sistemi di geolocalizzazione portati alla sua attenzio-

13

ne alla luce dell'aggiornato quadro normativo in materia di controlli a distanza, la cui osservanza costituisce condizione di liceità del trattamento dei dati personali (art. 4, l. n. 300/1970; artt. 11, comma 1, lett. *a*), e 114 del Codice). In relazione alla peculiarità di ciascun sistema tecnologico l'Autorità si è pronunciata sulla configurazione dello stesso quale strumento "dal quale derivi anche la possibilità di controllo a distanza" oppure quale strumento "utilizzat[o] dal lavoratore per rendere la prestazione lavorativa", con conseguente applicazione, rispettivamente, del comma 1 o 2 del menzionato art. 4 e quindi dell'obbligo o meno di attivare la procedura di garanzia ivi prevista.

Sotto tale ultimo profilo, in alcune decisioni il Garante ha ritenuto determinati sistemi non "direttamente preordinati all'esecuzione della prestazione lavorativa", con conseguente applicazione dell'art. 4, comma 1.

Al riguardo anche l'Ispettorato nazionale del lavoro, con circolare n. 2/2016, relativamente all'installazione di apparecchiature di localizzazione satellitare GPS su autovetture aziendali, ha chiarito che "in linea di massima e in termini generali […] i sistemi di geolocalizzazione rappresentano un elemento "aggiunto" agli strumenti di lavoro", e pertanto "le relative apparecchiature possono essere installate solo previo accordo con la rappresentanza sindacale ovvero, in assenza di tale accordo, previa autorizzazione dell'Ispettorato nazionale del lavoro".

Localizzazione dei veicoli per finalità di gestione, coordinamento e rendicontazione

Venendo ora ai singoli casi decisi, il Garante, con provvedimento reso in sede di verifica preliminare richiesta da una società che eroga servizi di fornitura di acqua potabile nonché di raccolta e trattamento delle acque reflue, ha precisato le condizioni di liceità del trattamento di dati di localizzazione dei veicoli aziendali, già oggetto del provvedimento di carattere generale del 4 ottobre 2011, n. 370 (provv. 16 marzo 2017, n. 138, doc. web n. 6275314).

Le finalità perseguite dal sistema sono risultate preordinate ad una pluralità di scopi, in particolare alla ottimizzazione della gestione delle attività aziendali in occasione di richieste di intervento o emergenze (conformemente ai livelli di garanzia e qualità delle prestazioni indicati dalla Carta dei servizi); all'innalzamento delle condizioni di sicurezza sul lavoro nonché della protezione della flotta aziendale in caso di furto; alla più efficiente programmazione delle attività sul territorio e degli interventi di manutenzione dei veicoli; all'effettiva commisurazione del tempo di lavoro; alla gestione di eventuali sinistri; alla gestione delle contestazioni di violazione amministrativa di disposizioni del codice della strada. Alla luce di tali finalità nonché delle modalità di funzionamento dei dispositivi, l'Autorità ha innanzitutto ritenuto il sistema di localizzazione dei veicoli non "direttamente preordinato all'esecuzione della prestazione lavorativa", con conseguente applicazione dell'art. 4, comma 1, l. n. 300/1970 (richiamato dall'art. 114 del Codice); in questa prospettiva i trattamenti sono stati ritenuti leciti, considerato altresì che la società aveva provveduto a stipulare accordi con le rappresentanze sindacali conformemente alla menzionata disciplina di settore in materia di controlli a distanza. Tuttavia, come misure a tutela dei diritti e delle libertà degli interessati, è stato prescritto alla società di configurare il sistema in modo da rilevare la posizione geografica con una cadenza temporale strettamente proporzionata alle finalità perseguite e in modo da consentire la conservazione dei dati trattati esclusivamente nelle ipotesi e con le modalità indicate in concreto nel provvedimento, in applicazione dei principi di protezione dei dati, distintamente per ciascuna finalità. Inoltre è stato precisato che il sistema deve essere configurato in modo da consentire l'accesso ai dati trattati esclusivamente al personale incaricato, al quale devono essere assegnate credenziali di autenticazione differenziate, individuando profili autorizzativi personalizzati e limitando quanto più possibile l'assegnazione di profili con funzionalità di modifica ed estrazione dei dati.

È stato altresì prescritto di adottare misure preordinate alla cancellazione automatica dei dati dopo la decorrenza degli eventuali termini di conservazione nonché di predisporre misure organizzative e tecnologiche volte ad anonimizzare i dati raccolti qualora ulteriormente utilizzati per finalità statistiche e di programmazione.

Con riferimento alla conservazione dei dati trattati, ove prevista, limitata ai dati strettamente necessari al perseguimento delle finalità perseguite, l'Autorità ha chiarito che "è in particolare escluso il monitoraggio dei tracciati percorsi".

All'esito della valutazione circa la liceità del trattamento, la sussistenza delle garanzie previste della disciplina sui controlli a distanza e le complessive caratteristiche del sistema (come sopra sommariamente riportate), il Garante ha individuato con il menzionato provvedimento, alla luce della disciplina sul cd. bilanciamento di interessi, un legittimo interesse del titolare al trattamento ai sensi dell'art. 24, comma 1, lett. *g*), del Codice.

Nell'ambito di una verifica preliminare presentata dal servizio di polizia locale di un comune, relativa alla prospettata installazione di un sistema di localizzazione satellitare sui veicoli e sulle radio ricetrasmittenti affidate al personale che svolge attività di polizia municipale e amministrativa anche per conto di tre comuni limitrofi, il Garante ha ritenuto lecite e coerenti con lo svolgimento delle funzioni istituzionali attribuite dall'ordinamento all'ente locale, le finalità di coordinamento e gestione di eventuali emergenze perseguite dal sistema attraverso la consultazione delle informazioni sulla posizione geografica di veicoli e dispositivi da parte del personale autorizzato addetto alla centrale operativa (provv. 19 ottobre 2017, n. 432, doc. web n. 7321142).

Parimenti lecito è stato ritenuto lo scopo di consentire la raccolta dei dati necessari alla rendicontazione delle attività effettuate dalle pattuglie nelle diverse aree comunali in vista della ripartizione tra i comuni dei costi sostenuti. Sotto il profilo della liceità, poi, anche in questo caso è stata ritenuta conforme alla disciplina in materia di controlli a distanza la preannunciata attivazione da parte del comune della procedura di garanzia prevista dall'art. 4, comma 1, l. n. 300/1970.

Quanto alla valutazione circa la necessità e proporzionalità delle modalità del prospettato trattamento, l'Autorità ha ritenuto conforme ai suindicati principi la possibilità di visualizzare in tempo reale sui *monitor* della sala operativa – da parte del responsabile del servizio (o di un suo delegato) – i dati raccolti in modo da non consentire la diretta identificazione degli operatori. Solo in caso di necessità il personale autorizzato potrà identificare e contattare i singoli operatori attraverso il raffronto con il registro cartaceo dei turni di servizio. Tale registro viene distrutto prima dell'inizio del nuovo turno, posto che in relazione agli scopi dell'ulteriore conservazione (consuntivazione dei costi relativi alle attività effettuate) non è necessaria (né comunque utile) l'identificazione degli operatori. Da ultimo si rileva che il Garante, in considerazione della assoluta peculiarità dell'attività svolta dalla polizia locale, ha ritenuto la periodizzazione temporale della posizione geografica effettuata dal sistema (pari a due rilevamenti al minuto) non in contrasto con il principio di proporzionalità.

In un altro caso, a seguito di istanza di verifica preliminare presentata da un gestore per conto di vari committenti (comuni o consorzi di comuni) dei servizi di igiene urbana (raccolta differenziata e trasporto rifiuti solidi urbani), ha formato oggetto di esame un sistema radiomobile digitale (dispositivi portatili e veicolari installati sulla flotta impiegata nel servizio erogato dalla società) per le comunicazioni del personale operativo (provv. 24 maggio 2017, n. 247, doc. web n. 6495708). Il Garante ha ritenuto che le finalità perseguite con il menzionato sistema, tra le quali l'ottimizzazione della gestione, il coordinamento e la sicurezza delle risorse sul

13

territorio, nonché la razionalizzazione del servizio in termini di copertura delle aree oggetto di intervento, fossero riconducibili alle "esigenze organizzative e produttive, per la sicurezza del lavoro e per tutela del patrimonio aziendale" in presenza delle quali la disciplina di settore in materia di controlli a distanza consente l'installazione di siffatti sistemi (artt. 11, comma 1, lett. *a*), e 114 del Codice nonché art. 4, comma 1, l. n. 300/1970).

In tale quadro è stata ritenuta correttamente attivata la procedura per l'acquisizione della specifica autorizzazione da parte della Direzione territoriale del lavoro competente (sul punto v. pure Ispettorato nazionale del lavoro, circolare n. 2/2016, ma già, seppur con riguardo al quadro normativo previgente, provv. 4 ottobre 2011, cit., punti 2.2. e 2.3). Sebbene infatti i dati di localizzazione del veicolo non fossero associati immediatamente ai lavoratori interessati, il datore di lavoro era in condizione di risalire alla loro identità (essendo ciascuno di essi, di volta in volta, assegnatario dei dispositivi e del veicolo nel quale gli stessi erano installati), ricostruendone così, anche indirettamente, l'attività (art. 4, comma 1, lett. *b*), del Codice; cfr., in proposito, provv. 4 ottobre 2011, cit., punto 1; parere n. 5/2005 del 5 novembre 2005 sull'uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto del Gruppo Art. 29, WP 115, p. 10; v. altresì parere n. 4/2007 sul concetto di dati personali, WP 136, p. 11).

Accanto al predetto sistema di geolocalizzazione la società intendeva inoltre implementare un "sistema di predisposizione turni" – configurato in modo da consentire, per ogni specifico servizio, l'assegnazione dei dispositivi (veicolari o mobili) ai dipendenti identificati nominativamente. Sebbene il sistema di geolocalizzazione non fosse idoneo a consentire un'associazione diretta tra le coordinate geografiche e i singoli operatori, la società poteva comunque associare i dipendenti ad un particolare dispositivo veicolare, per il tramite delle direzioni competenti, confrontando manualmente i *report* prodotti dai rispettivi sistemi, pur logicamente separati. La società aveva inoltre rappresentato l'intenzione di utilizzare tutti i dati, già raccolti ai sensi dell'art. 4, comma 1, l. n. 300/1970, e contenuti nei due distinti sistemi (rispettivamente quello di geolocalizzazione e quello di predisposizione dei turni), al fine di analizzarli per la risoluzione di eventuali "anomalie" nell'ambito della copertura del servizio e "a tutti i fini connessi al rapporto di lavoro".

Il Garante, nel rendere una prima applicazione della disposizione normativa di cui all'art. 4, comma 3, l. n. 300/1970, ha chiarito che anche tali ulteriori operazioni di trattamento devono essere effettuate nel rigoroso rispetto, sia della disciplina di protezione dei dati che di quella in materia di controlli a distanza. Sotto questo profilo, pertanto, è stato precisato che l'identificazione degli interessati può avvenire "solo in caso di necessità", "per scopi determinati, espliciti e legittimi" e a condizione che i dati siano utilizzabili "in altre operazioni di trattamento in termini compatibili con tali scopi", il trattamento ulteriore avvenga solo a fronte della concreta ricorrenza delle "anomalie", siano state predeterminate e rese note ai lavoratori unitamente alle modalità con le quali la società si riserva di trattare i dati e venga fornito agli interessati ogni informazione necessaria ad assicurare la piena consapevolezza dei trattamenti ulteriori che il datore di lavoro si riserva di effettuare e degli strumenti utilizzati (artt. 13 del Codice e 4, comma 3, l. n. 300/1970). Tali trattamenti potranno essere effettuati nei limiti della disponibilità dei dati personali trattati dal sistema di geolocalizzazione (in particolare, le coordinate geografiche ed il codice del dispositivo) in base a tempi di conservazione commisurati per il periodo strettamente necessario alla specifica finalità di consuntivazione del servizio.

Nel richiamare i propri consolidati orientamenti, il Garante ha ribadito che ogni operazione di trattamento ulteriore, ancorché effettuata nell'ambito della gestione

del rapporto contrattuale con il lavoratore e nell'esercizio del potere di verifica dell'effettivo adempimento della prestazione (artt. 2086, 2087 e 2104 c.c.), deve essere ispirata alla liceità, proporzionalità e gradualità nel trattamento dei dati evitando interferenze ingiustificate nella sfera privata dei lavoratori, pena l'inutilizzabilità dei dati stessi (art. 11, comma 2, del Codice; cfr. punto 5, provv. 13 luglio 2016, n. 303, doc. web n. 5408460; ancorché con riferimento al quadro normativo previgente, con riguardo alla non utilizzabilità del dato sulla geolocalizzazione acquisito in violazione di legge, v. Cass. civ., sez. lav., n. 19922/2016).

Il Garante ha prescritto alcune misure a tutela dei diritti e delle libertà degli interessati: in particolare che le interrogazioni di ambedue i sistemi siano consentite solo a un numero ridotto di incaricati operanti presso le competenti unità organizzative, i quali devono essere identificati mediante specifiche credenziali di autenticazione; che le interrogazioni dei due sistemi siano registrate, tramite un apposito *file* di *log* (riportante la data e l'ora dell'operazione, l'operazione effettuata, i codici dei dispositivi/veicoli visualizzati, l'identificativo dell'incaricato) nel rispetto del provvedimento del Garante del 27 novembre 2008 sugli amministratori di sistema; che il sistema venga configurato in modo da consentire la conservazione dei dati trattati in applicazione dei principi di protezione dei dati, distintamente per ciascuna finalità. In particolare, è stato prescritto di anonimizzare i *report* destinati ad essere messi nella disponibilità rispettivamente dell'ufficio turni (per la finalità di pianificazione dei turni e l'assegnazione delle priorità del servizio da parte del personale) e dell'ente affidatario del servizio (per la finalità di consuntivazione del servizio) in modo che in essi non ricorrano dati che siano, anche indirettamente, riconducibili agli interessati (ad es., codice veicolo, sul punto, provv. 2 ottobre 2014, n. 434, doc. web n. 3534543). I dati dei percorsi storicizzati potranno essere conservati, come richiesto nei capitolati tecnici per l'affidamento del servizio, solo se le informazioni relative alla localizzazione per l'intera flotta utilizzata siano state opportunamente anonimizzate (artt. 3 e 11, comma 1, lett. *e*), del Codice; e punto 3, provv. 4 ottobre 2011, cit.). Con riferimento alla frequenza della rilevazione dei dati di geolocalizzazione, il Garante ha prescritto, in sostituzione delle due rilevazioni al minuto prospettate dalla società, che il sistema sia configurato in modo che la rilevazione del dato di geolocalizzazione avvenga nel momento in cui l'automezzo giunge in prossimità di punti di raccolta predeterminati e precedentemente georeferenziati (cd. rilevazione ad eventi) per scongiurare il monitoraggio continuo della posizione del veicolo (artt. 3 e 11, comma 1, lett. *a*) e *d*), del Codice; sul punto, raccomandazione del 1° aprile 2015, CM/Rec(2015)5, sul trattamento di dati personali nel contesto occupazionale, par. 16; ma v. già Gruppo Art. 29, parere n. 13, 16 maggio 2011, sui servizi di geolocalizzazione su dispositivi mobili intelligenti, WP 185, p. 15 e, in senso analogo, punto 3, provv. 4 ottobre 2011, cit.). È stato inoltre prescritto che solo in presenza di predeterminate anomalie nella gestione di un servizio la società potrà prevedere l'attivazione della rilevazione in tempo reale della posizione geografica del mezzo quando quest'ultimo dovesse effettuare una sosta superiore a un tempo massimo individuato dalla società e comunque non inferiore a cinque minuti.

Localizzazione di *smartphone* o *tablet* in uso ai dipendenti

Il Garante ha autorizzato, nell'ambito di un procedimento di verifica preliminare avviato da una società, l'installazione di un sistema tecnologico completo di funzionalità di localizzazione geografica di dispositivi *smartphone* e *tablet* preordinato al miglioramento dell'efficacia della certificazione ai clienti dei risultati di un servizio di controllo sulla qualità della distribuzione di materiale pubblicitario all'interno delle cassette postali (es. volantini, *depliant* commerciali, etc.) (provv. 30 novembre 2017, n. 505, doc. web n. 7522639).

Anche in questo caso, alla luce delle finalità perseguite dalla società e delle concrete modalità del trattamento prospettato, l'Autorità ha ritenuto che il sistema deve ritenersi "non direttamente preordinato all'esecuzione della prestazione lavorativa", con conseguente applicazione dell'art. 4, comma 1, l. n. 300/1970. Sotto tale profilo il complessivo trattamento è stato ritenuto lecito considerato che la società aveva dichiarato di voler attivare la procedura di garanzia prevista dalla menzionata disciplina di settore in materia di controlli a distanza.

L'Autorità ha in particolare valutato positivamente le concrete caratteristiche del sistema alla luce dei principi di necessità e proporzionalità. Si segnala in particolare la prevista pseudonimizzazione dei dati del dipendente addetto al controllo di qualità e la scelta di configurare la rilevazione della posizione geografica del dispositivo non in base ad un intervallo temporale predeterminato bensì all'esito del comportamento attivo del dipendente/*controller* e solo nell'ambito temporale di riferimento della specifica attività programmata nel turno di lavoro. Inoltre ciascun supervisore potrà accedere al sistema esclusivamente per finalità di gestione, coordinamento e migliore organizzazione dell'attività e i rapporti consegnati ai clienti circa i risultati dell'attività svolta non potranno contenere dati identificativi dei dipendenti/*controller*, conformemente a quanto già affermato dall'Autorità (v. provv. 2 ottobre 2014, n. 434). I tempi di conservazione dei dati raccolti, individuati alla luce dei tempi medi di gestione di eventuali contestazioni da parte dei clienti (in dieci giorni), sono stati ritenuti conformi ai principi di necessità e proporzionalità.

All'esito della valutazione circa la liceità del trattamento, la sussistenza delle garanzie previste della disciplina sui controlli a distanza, le complessive caratteristiche del sistema (come in sintesi riportate), il Garante ha individuato, alla luce della disciplina sul cd. bilanciamento di interessi (ai sensi dell'art. 24, comma 1, lett. *g*), del Codice), un legittimo interesse del titolare al trattamento dei dati.

L'Autorità ha tuttavia prescritto l'adozione di specifiche misure volte ad impedire l'eventuale trattamento di dati presenti sui dispositivi non afferenti all'attività lavorativa e comunque privati, quali quelli tratti dalla posta elettronica o dalla navigazione in internet o relativi al traffico telefonico, considerato anche che la società intende consentire ai dipendenti l'uso dei dispositivi aziendali anche per fini personali. Sui dispositivi, infine, dovrà essere visualizzata un'icona per tutto il tempo in cui la funzionalità di localizzazione è attiva.

13.3. *Il trattamento dei dati personali mediante "altri strumenti": un sistema di gestione delle attese allo sportello*

Il Garante ha assunto un'altra importante decisione all'esito dell'esame di numerose segnalazioni e reclami da parte di organizzazioni sindacali e dipendenti nei confronti di un gestore del servizio postale con riguardo ad un sistema utilizzato per la gestione delle attese allo sportello (provv. 16 novembre 2017, n. 479, doc. web n. 7355533).

Il sistema consentiva al datore di lavoro, in qualità di titolare del trattamento per il tramite del personale abilitato e incaricato con diversi profili di accesso al sistema, operazioni di trattamento di dati, anche su base individuale, riferiti ai lavoratori addetti allo sportello. Il sistema consentiva la visualizzazione di dati identificativi dell'operatore, sia sui *display* collocati su ogni singola postazione di sportello dell'ufficio postale, sia su una *console* di monitoraggio, che rendeva possibile una consultazione in tempo reale (e in alcuni casi continuativa) anche di altre informazioni di dettaglio (ad es., disponibilità dello sportello e tempo medio di evasione dei *ticket*

serviti associati in via diretta al nominativo dell'operatore). Era inoltre effettuata la memorizzazione dei dati anche identificativi dell'operatore (nominativo) con possibilità di estrazione di reportistica.

L'Autorità ha attivato una complessa attività istruttoria che ha messo in evidenza alcuni profili di violazione della disciplina di protezione dei dati personali. In particolare è stato rilevato che la società non aveva reso ai dipendenti la dovuta informativa circa modalità e finalità delle operazioni di trattamento rese possibili dal sistema né all'interno delle informative individualizzate né con documenti informativi resi noti alla generalità dei dipendenti. La società si era limitata, infatti, a trasmettere una "documentazione descrittiva" alle sole organizzazioni sindacali che non recava gli elementi essenziali richiesti dalla legge (art. 13 del Codice).

Con il provvedimento che ha definito il procedimento il Garante ha ribadito che l'informativa ai sensi dell'art. 13 è dovuta indipendentemente dalla eventuale determinazione del titolare del trattamento di voler riservarsi di utilizzare le informazioni raccolte "a tutti i fini connessi al rapporto di lavoro" e che inoltre tali eventuali e successive operazioni di trattamento presuppongono il rigoroso rispetto della disciplina di protezione dei dati e di quella di settore in materia di controlli a distanza (provv. 24 maggio 2017, n. 247, doc. web n. 6495708, punto 5.3). Alla luce delle accertate caratteristiche, il Garante ha ritenuto il sistema non indispensabile all'operatore per rendere la prestazione lavorativa, "collocandolo" così fra quegli strumenti, anche organizzativi, dai quali può indirettamente derivare il controllo a distanza dell'attività dei lavoratori, con conseguente necessità di attivare le procedure concertativo/amministrative previste dalla legge (art. 4, comma 1, l. n. 300/1970 rispetto al comma 2; cfr. sul punto anche provv. 13 luglio 2016, n. 303, punto 4.3, doc. web n. 5408460).

Tali condizioni di garanzia, che costituiscono il presupposto di liceità del trattamento, non possono essere soddisfatte, come avvenuto nel caso di specie, con l'invio alle organizzazioni sindacali di un mero documento informativo o dall'eventuale acquiescenza dei lavoratori (cfr. Cass., III sez. pen., n. 22148/2017; sul punto, tra i tanti, provv. 8 maggio 2014, n. 230, doc. web n. 3250490). Pertanto, il trattamento che sarebbe derivato dal sistema in parola è stato ritenuto, anche sotto tale profilo, in contrasto con la disciplina in materia di protezione dei dati personali e con la rilevante disciplina di settore. Inoltre, alcune funzionalità del sistema, in particolare la possibilità in capo a specifiche funzioni aziendali, anche a livello centrale, di accedere in tempo reale e in via continuativa ai dati su base individuale relativi a tutte le postazioni e a tutti gli operatori in servizio in un dato momento presso un determinato ufficio, seppur nell'ambito di un'area territoriale definita, sono state ritenute non conformi ai principi di necessità, pertinenza e non eccedenza rispetto alle finalità "organizzative e produttive", "di sicurezza del lavoro" e "di tutela del patrimonio aziendale" consentite dalla richiamata disciplina di settore. Sotto questo profilo, il monitoraggio costante dell'attività e della produttività del lavoratore reso possibile dal sistema è stato ritenuto illecito (artt. 3, 11, comma 1, lett. *d*), del Codice e art. 4, l. n. 300/1970; raccomandazione Consiglio di Europa 1° aprile 2015, CM/Rec(2015)5, princ. 15; provv.ti 22 dicembre 2016, n. 547, par. 3.5, doc. web n. 5958296 e 13 luglio 2016, n. 303, par. 5, cit.).

Per tali ragioni il Garante ha disposto il divieto del trattamento con la conseguente inutilizzabilità dei dati trattati in violazione di legge, ai sensi dell'art. 11, comma 2 del Codice.

Con riguardo, invece, alla visualizzazione del nome di battesimo o dello pseudonimo del lavoratore sul *display*, quale diversa ed ulteriore misura rispetto a quella, peraltro già in uso per il personale operante a contatto con il pubblico, consistente

nell'apposizione del cartellino identificativo, il Garante ha ritenuto che la possibilità di raggiungere gli stessi legittimi obiettivi nei rapporti con i clienti con modalità diverse da quelle in uso potrà essere valutata, anche in alternativa al cartellino, previa idonea informativa ai lavoratori interessati, avuto riguardo, nel rispetto del principio di proporzionalità, alle dimensioni della struttura, al numero degli operatori che vi prestano servizio, alle mansioni svolte da ciascuno, al bacino di utenza del singolo ufficio postale, valutando l'opportunità di una rideterminazione dell'arco temporale di esposizione del nominativo dell'operatore.

13.4. *Il trattamento di dati personali mediante sistemi di videosorveglianza all'interno di aree particolari con rilevazione dell'audio*

Il Garante ha effettuato la valutazione di un sistema composto da apparecchiature preordinate alla registrazione di immagini e suoni all'interno di particolari aree tecniche delle navi da crociera gestite dalla società che ha presentato l'istanza di verifica preliminare (cd. *Engine control room*, sala di controllo dell'intero apparato motore della nave) (provv. 16 febbraio 2017, n. 62, doc. web n. 6164054).

In base alla vigente disciplina di rango nazionale, europeo e internazionale posta a protezione della sicurezza delle persone e dell'ambiente marino a fronte dei rischi connessi alle attività di trasporto marittimo, tutte le navi che fanno scalo nei porti nazionali devono essere dotate di un registratore dei dati di viaggio contenente, tra l'altro, la registrazione dell'audio delle conversazioni ed ogni altro suono captato da microfoni collocati sul ponte di comando.

A fronte della rappresentata necessità di innalzare i livelli di sicurezza, di consentire la ricostruzione di eventuali incidenti o anomalie nel funzionamento dei sistemi e l'individuazione di possibili fattori di rischio nelle procedure adottate, l'Autorità ha ritenuto di autorizzare un (analogo) sistema di raccolta dei dati anche all'interno della *Engine control room*, posto che l'attività che ivi si svolge è strettamente collegata a quella effettuata sul ponte di comando, anche alla luce delle caratteristiche tecnologiche della strumentazione di bordo.

All'esito della valutazione circa la liceità del trattamento, la sussistenza delle garanzie previste della disciplina sui controlli a distanza (anche in questo caso la società ha dichiarato di voler attivare la procedura prevista dall'art. 4, comma 1, l. n. 300/1970) e le complessive caratteristiche del sistema, il Garante ha riconosciuto con il provvedimento, alla luce della disciplina sul cd. bilanciamento di interessi (ai sensi dell'art. 24, comma 1, lett. *g*), del Codice), un legittimo interesse del titolare del trattamento dei dati.

Considerati i rischi specifici per i diritti e la libertà degli interessati connessi in special modo alla raccolta dei dati relativi all'audio, il Garante ha prescritto l'adozione di specifiche misure relative all'autenticazione dei soggetti autorizzati ad accedere al sistema (attribuzione di specifiche credenziali o dispositivi di autenticazione forte); al tracciamento degli accessi effettuati, che deve anche indicare i riferimenti temporali ed avere caratteristiche di completezza, integrità, inalterabilità e durata della conservazione analoghe a quelle richieste per i *log* degli accessi degli amministratori di sistema. È stata inoltre prescritta la cifratura delle registrazioni audio e video e la cancellazione irreversibile delle stesse decorsi i tempi di conservazione dei dati (individuati in 70 ore), tranne che in caso di verificazione degli eventi previsti (sinistri ed eventi anomali).

Visto, infine, che la società intende utilizzare alcune registrazioni per finalità didattico-formative, l'Autorità ha precisato che la necessaria previa anonimizzazione

dei dati dovrà riguardare anche le voci (provvedendo alla loro alterazione) e che si dovrà altresì eliminare qualunque elemento che possa ricondurre all'identità delle persone coinvolte (es: nomi, appellativi, riferimenti temporali espliciti).

13.5. *Il trattamento di dati biometrici*

A seguito di una segnalazione presentata al Garante da un dipendente civile del Ministero della difesa è emerso che per un lungo periodo di tempo l'amministrazione ha trattato dati biometrici (mediante estrazione del *template* dell'impronta digitale) di tutti i dipendenti – civili e militari, indipendentemente dalla mansione svolta – che hanno chiesto il rilascio o il rinnovo della Carta multiservizi della difesa (tessera di identificazione dei dipendenti anche per finalità di autenticazione all'accesso ai servizi forniti in rete con funzioni di carta nazionale dei servizi). Tale trattamento, secondo quanto dichiarato dall'amministrazione, era preordinato all'autenticazione dei soggetti specificamente autorizzati ad accedere alle aree della *Certification Authority*. Il Garante, all'esito di una complessa istruttoria, ha ritenuto illecito il trattamento sotto diversi profili (provv. 24 maggio 2017, n. 249, doc. web n. 6531525).

La disciplina sulla tessera di riconoscimento elettronica rilasciata dalle amministrazioni dello Stato prevede l'inserimento di dati personali, anche biometrici, previa attivazione di un procedimento di verifica preliminare dinnanzi al Garante ai sensi dell'art. 17 del Codice (art. 6, d.P.C.M. 24 maggio 2010, Regole tecniche delle tessere di riconoscimento (mod. AT) di cui al d.P.R. n. 851 del 1967 rilasciate con modalità elettronica dalle Amministrazioni dello Stato, ai sensi dell'art. 66, comma 8, d.lgs. n. 82/2005, modificato con d.P.C.M. 18 gennaio 2016). Inoltre, in base a tale disciplina, nell'ambito delle finalità proprie delle tessere di riconoscimento, l'amministrazione può utilizzare "per particolari esigenze di sicurezza fisica o logica […] informazioni biometriche come le impronte digitali […] del titolare dell'ATe. L'utilizzo di tali informazioni avviene nel rispetto della normativa in materia di protezione dei dati personali". È inoltre specificato che i dati biometrici possono essere inseriti nella tessera "per specifici scopi di sicurezza dell'amministrazione stessa" (all. B, d.P.C.M. cit., punti 3.1 e 6.2).

In materia di trattamento dei dati biometrici l'Autorità, in un'ottica di semplificazione, con il provvedimento generale prescrittivo in materia di biometria (12 novembre 2014, n. 513, doc. web n. 3556992) ha, tra l'altro, individuato alcune ipotesi per le quali – in presenza dei requisiti di legittimità previsti dal Codice nonché nel rispetto di determinate prescrizioni tecniche – il titolare del trattamento è esonerato dall'attivare l'istanza di verifica preliminare dinnanzi all'Autorità (v. in particolare punto 4.2, relativo al controllo dell'accesso fisico ad aree sensibili e all'utilizzo di apparati e macchinari pericolosi). Resta ferma la possibilità di trattare dati, anche biometrici, per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge (v. art. 58 del Codice).

Il trattamento effettuato dal Ministero della difesa non si inseriva entro tale cornice, sia perché i dati biometrici (nell'arco temporale sopra indicato) venivano raccolti e successivamente trattati nei confronti di tutti i dipendenti, senza alcuna selezione di coloro che avrebbero avuto accesso alle particolari aree destinate ad ospitare la *Certification Authority*, sia perché ai dipendenti non era stata fornita un'idonea informativa sulle caratteristiche fondamentali del trattamento; né, infine, l'amministrazione aveva provveduto ad effettuare la notificazione al Garante.

Il Garante, ritenuto illecito il trattamento, ha prescritto all'amministrazione di effettuare un programma di aggiornamento delle Carte multiservizi contenenti i

dati biometrici volto ad inibire il trattamento dei dati memorizzati in violazione delle disposizioni vigenti.

È stata invece accolta la richiesta di verifica preliminare finalizzata, nel rispetto delle procedure previste dallo Statuto dei lavoratori, alla conservazione fino a trenta giorni delle immagini registrate dal sistema di videosorveglianza e dei dati rilevati dal sistema di controllo accessi biometrico, basata su oggettive esigenze di sicurezza, da parte di una società proprietaria di un complesso immobiliare adibito a centro orafo in cui sono ubicati immobili di proprietà delle imprese socie e spazi ad uso comune di proprietà esclusiva della società consortile che provvede inoltre alla gestione di tutte le attività di servizi e di impresa necessarie (vigilanza, custodia, sicurezza, tutela, pulizia, manutenzione, ristorazione) (provv. 20 aprile 2017, n. 198, doc. web n. 6393088).

13.6. *Il trattamento di dati giudiziari*

Nel 2017 il Garante si è pronunciato rispetto ad alcune richieste di autorizzazione al trattamento di dati giudiziari in ambito di lavoro (artt. 27 e 41 del Codice).

Fra i casi esaminati, si menziona una richiesta di una società che gestisce in appalto servizi di pulizie nel settore dei trasporti ferroviari rispetto ai dati giudiziari dei propri dipendenti con funzioni di "manovale e pulitore di impianti fissi" a bordo dei treni (provv. 15 giugno 2017, n. 267, doc. web n. 6558837).

In particolare la società ha chiesto di poter acquisire il certificato del casellario giudiziale consegnato dai medesimi dipendenti e di fornirne copia alla società appaltante. La società ha infatti motivato la richiesta con la necessità di conformarsi a quanto previsto da uno schema di contratto di appalto, non ancora stipulato, il quale prevedrebbe per l'appunto l'impegno dell'appaltatore a raccogliere il certificato generale del casellario nonché a "segnalare tempestivamente al committente il nominativo di coloro a carico dei quali risultano sentenze di condanna passate in giudicato nonché i reati ascritti e la pena comminata".

Con l'autorizzazione generale n. 7 del 2016 il Garante, conformemente a quanto previsto dall'art. 27 del Codice, ha autorizzato i datori di lavoro al trattamento dei dati giudiziari qualora ciò sia "indispensabile per […] adempiere o esigere l'adempimento di specifici obblighi o eseguire specifici compiti previsti da leggi, dalla normativa dell'Unione europea, da regolamenti o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro".

Il Garante ha ritenuto insussistente nel caso concreto un'idonea base giuridica – legislativa, regolamentare o contrattuale – per il trattamento nell'ambito del rapporto di lavoro da parte della società richiedente di informazioni così delicate (considerato che il certificato generale del casellario contiene il riferimento ai provvedimenti di condanna definitivi, in relazione a qualsiasi tipologia di fattispecie di reato, nonché la menzione di alcuni provvedimenti definitivi in materia civile ed amministrativa), né in relazione alla prospettata comunicazione dei dati alla società appaltante. L'Autorità, per tali motivi, ha rigettato la richiesta di autorizzazione.

Un'altra richiesta ai sensi dell'art. 41 del Codice – pervenuta da una società, a tutela propria e delle numerose amministrazioni per conto delle quali opera in settori altamente strategici per il Paese – ha riguardato la possibilità di richiedere, direttamente e a campione, il certificato penale del casellario giudiziale di un centinaio di dipendenti, posti in posizione apicale e in ruoli chiave all'interno dell'azienda. Nell'accoglierla, l'Autorità ha ritenuto che il trattamento dei dati giudiziari fosse necessario per lo svolgimento delle funzioni e degli specifici servizi erogati in

ambito pubblico dalla società, che tratta volumi rilevanti di dati personali rivestendo un ruolo centrale nel processo di digitalizzazione e di interoperabilità tra le pp.aa. (anche mediante servizi integrati). In particolare, il trattamento è stato autorizzato per le rilevanti finalità di interesse pubblico perseguite, tra le quali rientra la necessità di assicurare elevati livelli di sicurezza, tenuto conto della delicatezza nonché del volume dei dati trattati, anche mediante l'accertamento dei requisiti di affidabilità e onorabilità del personale cui sono assegnati incarichi o funzioni di particolare rilevanza e "sensibilità" all'interno della società. Il Garante ha prescritto alla società di informare il personale della possibilità della verifica e di definire l'ambito oggettivo del trattamento, individuando tassativamente il novero delle fattispecie di reato oggetto di verifica rispetto alle finalità perseguite (ed esplicitate), con riguardo a reati di particolare gravità, tali da incidere sui profili di onestà e di correttezza del dipendente in relazione alle specifiche funzioni o mansioni a questi assegnate; in tale prospettiva la valutazione deve incentrarsi sui delitti contro il patrimonio e la personalità interna dello Stato (provv. 19 gennaio 2017, n. 10, doc. web n. 5953097).

13.7. *Il trattamento di dati sanitari di familiari e congiunti del dipendente a fini di fruizione di permessi e congedi*

Con segnalazione presentata da un'organizzazione sindacale è stato lamentato che una società operante nel settore delle telecomunicazioni richiedesse ai propri dipendenti la produzione di certificazione sanitaria contenente anche "elementi costituenti la diagnosi clinica" riferiti a terzi rispetto al rapporto di lavoro in applicazione della normativa di settore secondo cui la documentazione medica che deve essere presentata dal dipendente al proprio datore di lavoro ai fini della fruizione dei permessi retribuiti per "grave infermità" del coniuge, parenti o conviventi e dei congedi non retribuiti "per gravi motivi familiari" (art. 4, commi 1 e 2, l. 8 marzo 2000, n. 53 e artt. 1 e 2, comma 1, lett. *d*), d.m. 21 luglio 2000, n. 278). In particolare, è stato accertato che la società chiedeva ai propri dipendenti, quale condizione per la fruizione del beneficio (consistente in permessi giornalieri o periodi di congedo), la produzione di certificazione sanitaria contenente sia l'attestazione della condizione di "grave infermità", espressamente richiesta dalla legge, sia la descrizione degli elementi costituenti la diagnosi clinica, peraltro riferita a soggetti terzi rispetto al rapporto di lavoro ("documentata grave infermità del coniuge o di un parente entro il secondo grado o del convivente, purché la stabile convivenza con il lavoratore o la lavoratrice risulti da certificazione anagrafica"; art. 4, comma 1, l. 8 marzo 2000, n. 53, cit.). A seguito di una complessa attività istruttoria, tenuto conto di una pluralità di segnalazioni, istanze e quesiti in merito al medesimo comportamento posto in essere in altri contesti lavorativi nonché del generale impatto nell'ambito della gestione del rapporto di lavoro, sia pubblico che privato, sono stati effettuati approfondimenti con il Ministero del lavoro e delle politiche sociali, il quale ha rappresentato il proprio orientamento e i necessari chiarimenti in merito alla portata applicativa di alcuni propri precedenti interpretativi.

Nel definire il procedimento con nota del 19 ottobre 2017, l'Autorità ha dichiarato che la condotta del datore di lavoro non risultava conforme alla disciplina di protezione dei dati personali (artt. 3, 11, comma 1, lett. *d*), e 26 del Codice e autorizzazioni generali nn. 1 e 2 cit.; cfr., tra i tanti, provv. 21 marzo 2007, doc. web n. 1395821 e, anche, provv.ti 21 aprile 2009, doc. web n. 1616870; 9 novembre 2005, doc. web n. 1191411).

13

L'Autorità ha in proposito ribadito che il trattamento dei dati da cui si possa desumere lo stato di malattia o l'esistenza di patologie dei soggetti interessati può essere effettuato dal datore di lavoro nell'ambito della finalità di gestione del rapporto di lavoro, nel rispetto della disciplina di protezione dei dati personali; e ciò, anche ove i dati siano riferiti a soggetti terzi individuati dalla legge (art. 433 c.c.), come ad esempio i congiunti o conviventi del lavoratore (artt. 3, 11 e 26, comma 4, lett. *d*), del Codice, e autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro – n. 1/2016, n. 523, doc. web n. 5800451, punto 3), lett. *a*) e *b*) nonché autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale – n. 2/2016, n. 424, doc. web n. 5803257, punto 1.3, lett. *b*); cfr. anche linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati, n. 53 del 23 novembre 2006, doc. web n. 1364099, punto 6.4).

La disciplina di protezione dei dati personali richiede in ogni caso l'osservanza dei princìpi di necessità, proporzionalità e indispensabilità, che impongono al datore di lavoro di valutare specificamente il rapporto tra i dati oggetto di trattamento e gli adempimenti derivanti da compiti e obblighi di volta in volta previsti dalla normativa di settore, e di adottare soluzioni che, pur consentendo di svolgere gli adempimenti in modo efficace, eliminino ogni occasione di superflua conoscibilità dei medesimi da parte di soggetti non legittimati al trattamento (cfr. artt. 3 e 11, comma 1, lett. *d*), del Codice; aut. gen. n. 1/2016, punto 5 e n. 2/2016, punto 3). In attuazione dei richiamati princìpi, pertanto, il datore di lavoro non può venire a conoscenza di tutti i dati sanitari del congiunto del lavoratore (diagnosi o anamnesi).

Come già chiarito negli altri casi di fruizione di permessi riconosciuti dalla legge per causali connesse allo stato morboso o di disabilità di un familiare, il lavoratore deve presentare al datore di lavoro una certificazione dalla quale risulti esclusivamente l'accertata condizione di volta in volta richiesta dalla legge. In altre parole, il perseguimento dei compiti e delle attribuzioni degli uffici preposti alla gestione del personale, destinatari della predetta documentazione, può ugualmente essere conseguito mediante l'acquisizione di una certificazione medico-legale attestante la sola sussistenza delle "grave infermità" o la ricorrenza di uno dei "gravi motivi familiari"; ciò consentirebbe l'effettuazione delle dovute verifiche da parte degli uffici destinatari della predetta documentazione in merito alla ricorrenza dei presupposti per il riconoscimento del beneficio, evitando al contempo la conoscibilità di informazioni sanitarie non indispensabili (sul punto, v. raccomandazione CM/REc (2015)5 sul trattamento dei dati personali nel contesto occupazionale, punto 9.7; Cass. civ., sez. lav., n. 2803/2015).

In conclusione l'Autorità ha precisato che è onere del lavoratore consegnare l'"idonea documentazione" di cui all'art. 3, d.m. n. 278/2000 al datore di lavoro quale condizione indefettibile per comprovare il proprio diritto e ottenere i benefici in esame e che, nell'attestare la sola sussistenza della "grave infermità" o la ricorrenza di uno dei "gravi motivi familiari", potrà specificare, ad esempio, se la patologia sia "acuta o cronica" e se sia direttamente riconducibile ad una delle situazioni patologiche individuate tassativamente ai punti da 1 a 4 della lett. *d*) dell'art. 2 del citato decreto, ma dovrà comunque essere priva dell'indicazione della specifica patologia diagnosticata all'interessato, con l'omissione delle parti dedicate alla descrizione dei dati anamnestici, all'esame obiettivo e alla diagnosi della persona (analoga considerazione vale per la certificazione da esibire nei casi di "grave infermità", trattandosi, come chiarito in più occasioni dal Ministero del lavoro e delle politiche sociali, di una *species* rispetto al *genus* dei "gravi motivi", di cui le patologie enumerate dal regolamento costituiscono cd. figure sintomatiche; art. 4, comma 2, l. n. 53/2000 e art. 2, comma 1, lett. *d*), d.m. n. 278/2000).

14 Le attività economiche

14.1. *Il settore bancario*

Il numero di segnalazioni, reclami, quesiti e richieste di parere pervenute all'Autorità nel 2017 in materia di trattamento di dati personali della clientela in ambito bancario è stato particolarmente consistente.

Parte di esse hanno riguardato profili sui quali il Garante si era già espresso in passato, tra l'altro con le linee guida adottate con il provvedimento del 25 ottobre 2007, n. 53 (doc. web n. 1457247) e con il provvedimento generale recante prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (provv. 12 maggio 2011, n. 192, doc. web n. 1813953).

Altre hanno riguardato il trattamento dei dati personali effettuato dagli istituti di credito in occasione delle operazioni di adeguata verifica della clientela prescritte dalla vigente normativa in materia di antiriciclaggio. Su tale complessa e delicata disciplina, peraltro, il Garante si è espresso nel 2017, rendendo il proprio parere (provv. 9 marzo 2017, n. 125, doc. web n. 6124534) sullo schema di decreto legislativo adottato in recepimento della direttiva (UE) 2015/849 del Parlamento e del Consiglio del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (cd. quarta direttiva).

Sempre in relazione alle varie questioni affrontate dal Garante con le linee guida del 2007, sono state esaminate e definite numerose istanze, in particolare, sui profili dell'accesso ai dati personali contenuti in rapporti bancari (di norma, libretti di risparmio, conti correnti e depositi titoli) riferiti a persone decedute, della richiesta di copia di documentazione riferita a rapporti bancari e della comunicazione a terzi di dati inerenti clienti.

In particolare, l'adozione, da parte di un noto istituto di credito, delle misure previste dal provvedimento in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie ancora prima della sua effettiva operatività ha consentito all'Autorità, ancora una volta, di pronunciarsi in favore di una cliente che aveva segnalato l'illiceità della comunicazione a un soggetto terzo non autorizzato di dati personali attinenti al suo conto corrente (provv. 22 giugno 2017, n. 286, doc. web n. 6629414). Nonostante, infatti, da un primo accertamento non fossero emerse anomalie, a seguito di un ulteriore approfondimento richiesto dall'Autorità su un maggior numero di filiali e prendendo in esame un arco temporale più ampio, è risultato che un dipendente aveva effettivamente posto in essere una serie di accessi indebiti al conto corrente della segnalante da filiali diverse da quella di appartenenza e senza apparenti motivazioni operative.

14.2. *Le banche dati interoperatore e i codici di deontologia nel settore economico/finanziario*

14.2.1. I lavori di revisione del cd. codice Sic

In occasione degli incontri tenutisi durante l'anno con gli operatori convolti, sono emerse posizioni estremamente contrastanti, tali da compromettere la possibi-

lità di concludere positivamente l'intrapreso percorso di revisione del codice di deontologia e buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti (cd. codice Sic), iniziativa di cui si era dato conto nella Relazione 2016 (p. 106).

Constatate le difficoltà di addivenire ad una positiva chiusura dei lavori da tempo intrapresi e preso atto della necessità e improcrastinabilità di alcuni chiarimenti, almeno sulle disposizioni del codice deontologico che generavano da tempo considerevoli dubbi interpretativi e applicativi (un indicatore in questo senso è dato dal moltiplicarsi, nel corso degli ultimi anni, di richieste di intervento rivolte all'Autorità), il Garante ha adottato il provvedimento 26 ottobre 2017, n. 438 (doc. web n. 7221677).

Con tale decisione, facendo anche propri gli orientamenti più recenti della Corte di cassazione (Sez. I civ., ord., 13 giugno 2017, n. 14685), l'Autorità ha affermato che gli istituti di credito e gli operatori finanziari non bancari hanno l'obbligo di inviare, ai soggetti che siano in ritardo nei pagamenti delle rate di un contratto di finanziamento o di un mutuo, il preavviso di imminente registrazione nei sistemi di informazioni creditizie (prescritto dall'art. 4, comma 7, del codice di deontologia) usando modalità idonee a provarne l'avvenuta ricezione da parte degli interessati (a titolo esemplificativo, tramite raccomandata con ricevuta di ritorno, telegramma o posta elettronica certificata).

Sui tempi di conservazione nei sistemi di informazioni creditizie dei dati relativi a inadempimenti non regolarizzati, il Garante ha precisato che, fermo restando il termine per così dire ordinario di 36 mesi dalla scadenza contrattuale o dalla cessazione del contratto, negli altri specifici casi previsti dall'art. 6, comma 5, del codice di deontologia (cioè in caso di altre vicende rilevanti in relazione al pagamento quali, a titolo esemplificativo, la cessione del rapporto a società di recupero crediti, o la cessione in blocco e cartolarizzazione dei crediti), il tempo di conservazione non può comunque mai superare i 5 anni dalla data di scadenza del contratto.

Sulla cd. informativa personalizzata "SECCI" - *Standard european consumer credit information* (prevista dall'art. 124 del Testo unico bancario e che costituisce uno strumento mediante il quale il finanziatore informa l'interessato – non solo prima che questi sia vincolato da un contratto, ma addirittura prima che abbia formulato una richiesta di finanziamento – sulle condizioni del finanziamento), il Garante ha chiarito che il codice deontologico si applica solo in presenza di un rapporto di credito già instaurato, o quanto meno di una richiesta volta alla conclusione del medesimo, mentre non può trovare applicazione nella fase antecedente alla formulazione di una richiesta di finanziamento (di norma coincidente con il momento in cui l'interessato si rivolge ad un istituto di credito o ad un operatore finanziario non bancario per ottenere un preventivo, al fine di valutare la convenienza a formalizzare una richiesta di finanziamento). In tale fase, banche e finanziarie devono tener conto esclusivamente delle informazioni rese, direttamente e spontaneamente, dal consumatore, senza possibilità di consultare i sistemi di informazione creditizia.

14.2.2. Altre ipotesi di banche dati interoperatore

Al di là del codice Sic di cui si è detto (e di altre banche dati strutturate quali quelle delle società che operano nel settore delle informazioni commerciali), si è intensificata, nei più vari settori economici, la richiesta di costituzione di banche dati settoriali miranti a contenere i rischi legati alla gestione dei rapporti contrattuali o a prevenire azioni fraudolente.

Con provvedimento 20 aprile 2017, n. 199 (doc. web n. 6407608), il Garante ha rigettato la richiesta di bilanciamento di interessi presentata da una società spe-

cializzata nella riparazione e sostituzione di cristalli degli autoveicoli. Tale società, liquidataria diretta degli interventi eseguiti a beneficio degli assicurati di alcune compagnie assicurative convenzionate, avrebbe voluto rendere disponibile a queste ultime, quale servizio aggiuntivo, una piattaforma web preordinata alla raccolta e all'elaborazione di informazioni utili a verificare eventuali richieste di risarcimento danni fraudolente (perché collegate, nei casi indicati, a denunce artatamente postdatate); ciò, invero, senza richiedere il consenso degli interessati, ritenuto di difficile acquisizione anche alla luce delle finalità dichiaratamente perseguite.

Il Garante, nel puntualizzare che le attività di prevenzione e contrasto di fenomeni fraudolenti nel settore assicurativo sono disciplinate, anzitutto, per via legislativa, attraverso la costituzione di banche di dati gestite da soggetti pubblici, ha escluso che i rapporti di collaborazione intercorrenti tra la società istante e le compagnie di assicurazione potessero costituire, ai fini della richiesta di bilanciamento di interessi avanzata, un'idonea base giustificativa. Ferma restando, peraltro, l'indimostrata sussistenza di ragioni atte a ritenere come minusvalenti i diritti o le libertà degli interessati rispetto all'interesse perseguito dal titolare o da terzi destinatari dei dati, l'Autorità ha poi sottolineato come la piattaforma in esame avrebbe consentito il censimento anche di soggetti non necessariamente animati da intenti fraudolenti, con il rischio di comprimere le possibilità per questi ultimi di stipulare polizze del tipo qui considerato.

Con provvedimento 30 novembre 2017, n. 502 (doc. web n. 7355034), il Garante ha invece accolto una richiesta di verifica preliminare relativa al trattamento di dati personali connesso alla costituzione di una banca di dati nel settore dei veicoli a noleggio. Facendo seguito al provvedimento adottato in data 1° giugno 2016, n. 234 (doc. web n. 5306512), con cui l'Autorità aveva rilevato alcune criticità nel trattamento dei dati derivante dall'istituzione della banca di dati precedentemente prefigurata, l'Associazione nazionale industria dell'autonoleggio e servizi automobilistici - Aniasa (organizzazione rappresentativa delle imprese operanti nel settore dell'autonoleggio a breve e lungo termine) ha presentato una nuova richiesta di verifica preliminare corredata, oltre che da sostanziali modifiche al prospettato *database*, da ulteriori elementi di valutazione e motivazioni non addotti nel corso della pregressa istruttoria. Nel rimodulare significativamente i presupposti per l'iscrizione nella banca dati, prevedendo altresì meccanismi di filtraggio e verifica delle informazioni inserite, l'associazione ha circoscritto notevolmente il novero dei dati suscettibili di censimento (escludendo, tra l'altro, quelli sensibili e giudiziari, nonché quelli identificativi di persone vittime di furti di identità), limitandone l'utilizzabilità ai soli fini previsti. Rassicurazioni sono state inoltre fornite in merito all'utilizzo dei dati da parte delle singole società di autonoleggio, nonché ai rigorosi controlli che la stessa Aniasa si è impegnata a effettuare sulle società partecipanti.

Nel valutare positivamente l'istanza, il Garante, pur ribadendo l'opportunità di evitare proliferazioni indiscriminate di archivi settoriali nei più disparati ambiti economici, ha ritenuto che nel settore in esame potesse eccezionalmente prevedersi la costituzione di una banca di dati come quella descritta, in ragione delle specificità del settore medesimo e della peculiarità dei servizi offerti, nonché dei numerosi e onerosi rischi gravanti sulle società di autonoleggio, tali da compromettere, secondo quanto riferito, l'ordinario svolgimento delle attività del comparto, condizionando fortemente le strategie di mercato e le politiche occupazionali dei singoli operatori economici. Anche in considerazione dei molteplici danni già subiti dal settore e della necessità di ridurre i suddetti rischi, si sono inoltre ritenuti sussistenti i presupposti per effettuare un bilanciamento di interessi in relazione allo specifico trattamento di dati personali connesso al sistema in esame (art. 24, comma 1, lett. *g*), del Codice).

14.3. *La videosorveglianza in ambito privato*

Con provvedimento 21 dicembre 2017, n. 551 (doc. web n. 7496252), il Garante ha ritenuto lecito il trattamento effettuato da Grandi Stazioni Retail s.p.a., in relazione all'istallazione di numerosi impianti pubblicitari digitali (colonnine pubblicitarie), con finalità di analisi dell'*audience* pubblicitaria, già presenti presso alcune aree di frequente passaggio del pubblico all'interno delle principali stazioni ferroviarie, ammettendone la prosecuzione a condizione dell'adempimento di alcune prescrizioni.

A seguito dell'istruttoria svolta dall'Autorità, è stato appurato che tali impianti, dotati di uno schermo sul quale vengono trasmessi messaggi pubblicitari ed informazioni predeterminate, sono forniti di sensori in grado di effettuare la raccolta di dati di *audience* per valutare l'efficacia della comunicazione pubblicitaria trasmessa. La raccolta di tali dati, effettuata mediante l'utilizzo di un'applicazione specifica, consentirebbe di analizzare le immagini raccolte dal sensore video installato sulla colonnina (in genere una *webcam*) al fine di determinare la presenza di un volto umano nell'area ripresa, rilevarne il tempo di permanenza di fronte alla pubblicità – fornendo anche alcune informazioni (per quanto con un certo grado di approssimazione) desunte dalle caratteristiche del volto quali: sesso, fascia d'età, distanza dalla colonnina – effettuando infine analisi di tipo statistico volte ad individuare il livello di gradimento dei diversi messaggi pubblicitari.

La presenza di un volto verrebbe rilevata attraverso algoritmi di *face detection* e non di *face recognition* che consentirebbero quindi di captare (genericamente) la presenza di un volto umano senza però identificarlo attraverso caratteristiche biometriche.

Tali dati sarebbero cifrati e quindi memorizzati centralmente per effettuare analisi statistiche riferite al gradimento dei messaggi pubblicitari trasmessi.

Le immagini relative ai passanti non verrebbero invece salvate localmente nell'apparato né in alcun sistema della Società, ma solamente memorizzate nella memoria RAM dell'apparato locale per qualche decimo di secondo al massimo, venendo quindi subito sovrascritte dalle immagini successive.

Anche in questo caso il Garante ha indicato al titolare la necessità di adottare misure ed accorgimenti a tutela dei diritti degli interessati ed, in particolare, di predisporre un'informativa *ad hoc* in forma semplificata, ai sensi dell'art. 13, comma 3, del Codice, nonché di adottare le misure necessarie per implementare un monitoraggio periodico, con frequenza almeno semestrale, sullo stato dei dispositivi. Ciò per evidenziare eventuali malfunzionamenti, indisponibilità degli apparati o tentativi di accesso fraudolento, in ragione del rischio specifico relativo ad un possibile utilizzo di tali dispositivi da parte di un soggetto non legittimato.

Con provvedimento 14 dicembre 2017, n. 529 (doc. web n. 7450667), l'Autorità ha accolto la richiesta, ai sensi dell'art. 17 del Codice, presentata da una società che fornisce soluzioni di installazione, manutenzione, assistenza tecnica e *service*, in riferimento ad impianti e tecnologie di produzione di energia al fine di conservare sino a 6 mesi le immagini registrate dai propri sistemi di videosorveglianza installati all'interno di ogni singolo *container* (*tool container*) atto alla custodia, trasporto, stoccaggio di attrezzature sofisticate e di pregio, di proprietà della società stessa, dedicate alla manutenzione meccanica, elettrica e alla ricerca guasti, su cantieri di lavoro temporanei in Italia e all'estero. Tale decisione ha trovato giustificazione in obiettive esigenze di tutela del patrimonio aziendale non essendo risultato, il richiesto allungamento, né eccessivo né sproporzionato in relazione ai tempi tecnici necessari alla società per effettuare le opportune verifiche degli illeciti e delle giacenze.

Con un altro provvedimento il Garante ha accolto la richiesta di estensione, fino a 120 giorni, dei tempi di conservazione delle immagini presentata, ai sensi dell'art. 17, del Codice, da un istituto di vigilanza privata che svolge servizi di gestione, custodia e autenticazione del denaro al fine della re-immissione in circolo della moneta, all'esito dei controlli sull'idoneità della stessa a fungere da mezzo di scambio di beni e servizi.

Il sistema di videosorveglianza installato dalla Società è finalizzato a garantire la sicurezza del patrimonio aziendale e delle sedi aziendali che rappresentano un obiettivo sensibile in ragione dell'elevatissima quantità di valori che ivi vengono custoditi e riprende l'intero percorso del denaro all'interno dei locali aziendali.

L'Autorità ha ritenuto conforme ai principi di cui agli artt. 3 e 11, del Codice l'istanza di prolungamento del termine di conservazione delle immagini fino a 120 giorni in ragione delle esigenze di sicurezza, di tutela del patrimonio dei soggetti che affidano il denaro per le operazioni di custodia e di contazione, di tutela della correttezza delle operazioni svolte dalla società di vigilanza nonché di tutela della fiducia che il pubblico deve mantenere rispetto alla moneta in corso legale (provv. 9 novembre 2017, n. 462, doc. web n. 7457920).

14.4. *Attività imprenditoriali: esonero dall'informativa*

Il Garante è intervenuto con riferimento a due istanze di esonero dall'obbligo di rendere individualmente l'informativa agli interessati (ai sensi dell'art. 13, comma 5, lett. *c*), del Codice).

La prima ha riguardato un caso di cessione di ramo di azienda, connesso allo svolgimento di attività destinate alla gestione di catene di negozi e implicante il trattamento di dati personali di dipendenti, fornitori e clienti della società cedente. In particolare, l'istanza era stata formulata con riferimento agli interessati coinvolti in programmi di fidelizzazione posti in essere a suo tempo dalla società cedente, non contattabili però via *e-mail*, in quanto gli stessi, in sede di adesione al relativo programma, non avevano fornito il proprio indirizzo di posta elettronica.

Al riguardo – come già sostenuto in altre occasioni (provv. 11 giugno 2015, n. 347, doc. web n. 4169456) – il Garante 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 della nuova società 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. Resta 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).

In conclusione, dopo aver verificato l'impossibilità di rendere l'informativa a tutti gli interessati in forma individuale in ragione della natura sproporzionata dei mezzi che tale adempimento avrebbe comportato, il Garante ha accolto la richiesta di esonero, ai sensi dell'art. 13, comma 5, lett. *c*), del Codice, prescrivendo specifiche modalità alternative e semplificate, quali: la pubblicazione di un annuncio

recante i contenuti dell'informativa sui siti web delle società interessate; l'affissione dell'informativa completa presso i locali dei negozi, nonché la comunicazione della stessa agli interessati in occasione della prima circostanza utile di contatto (provv. 9 novembre 2017, n. 460, doc. web n. 7489156).

Con riguardo alla seconda istanza, l'esonero dall'obbligo di rendere individualmente l'informativa ha riguardato i dati dei clienti intestatari degli autoveicoli prodotti dalla società richiedente, già presenti in un *database* accessibile solo alla stessa, in relazione alla migrazione dei predetti dati ad un nuovo sistema informatico, sempre gestito dalla società, ma accessibile anche ad altri soggetti (tra cui concessionari, rivenditori auto e officine autorizzate) in *partnership* con la prima (cd. rete). L'istanza è stata giustificata in virtù della manifesta sproporzione, rispetto ai diritti tutelati, dei mezzi che la società avrebbe dovuto impiegare per fornire un'informativa in forma individualizzata; ciò tenuto conto sia del numero ingente di soggetti ai quali la stessa doveva essere fornita, sia degli elevati costi che la società avrebbe dovuto sostenere per trasmettere individualmente l'informativa in forma cartacea o via *e-mail*. Con il suddetto provvedimento di esonero, il Garante ha preso atto che la condivisione dei dati è stata prevista esclusivamente per finalità connesse all'adempimento di obblighi di legge (ad es. campagne di richiamo), di esecuzione di obblighi contrattuali (ad es. finalizzazione dell'ordine di acquisto, interventi in garanzia) nonché della cd. informativa precontrattuale (identificazione del cliente che si sia recato presso uno dei membri della rete al fine di meglio soddisfare le richieste del cliente medesimo: ad es., rilevazione dei dati del veicolo da riparare e della data dell'ultimo intervento; comunicazioni in merito alla data del successivo *test drive* ecc.) e ha tenuto conto dell'impegno assunto dalla società di pubblicare sui propri siti web un'unica informativa contenente gli estremi identificativi di tutti i titolari del trattamento e gli altri elementi previsti dall'art. 13, commi 1 e 2, del Codice. Inoltre, il Garante ha ritenuto di prescrivere, quali ulteriori misure opportune: ai membri della rete, la pubblicazione sui propri siti web dell'informativa prevista dall'art. 13 del Codice e l'affissione presso i propri locali della medesima informativa, dandone comunicazione agli interessati in occasione della prima circostanza utile di contatto; alla società, di tenere costantemente aggiornato su propri siti web l'elenco dei soggetti facenti parte della rete medesima, che agiscano in qualità di titolari del trattamento (provv. 5 luglio 2017, n. 302, doc. web n. 6845231).

14.5. *Attività imprenditoriali e nuove tecnologie*

Il Garante ha accolto la richiesta di verifica preliminare presentata, ai sensi dell'art. 17 del Codice, da una nota società produttrice di gioielli in relazione all'implementazione di un impianto biometrico con riconoscimento facciale finalizzato a garantire l'ingresso allo stabilimento produttivo esclusivamente al personale autorizzato. La società ha dichiarato che il sistema di controllo accessi prescelto consentirà di avere "contezza certa" dell'identità del personale presente all'interno dello stabilimento, garantendo un elevato livello di tutela dei beni e delle persone dal pericolo di furti e rapine, ma anche da possibili violazioni del marchio e del *copyright*. Il sistema non verrà utilizzato per finalità di rilevazione delle presenze del personale, ma avrà come unica finalità la tutela dell'incolumità dei dipendenti e della sicurezza del patrimonio aziendale (provv. 16 febbraio 2017, n. 60, doc. web n. 6136705).

Con provvedimento del 30 marzo 2017, n. 167 (doc. web n. 6407700) l'Autorità ha accolto la richiesta presentata ai sensi dell'art. 17 del Codice in relazione al trattamento dei dati personali connesso all'attivazione di una nuova funziona-

lità di localizzazione di telefoni cellulari o altri strumenti (*device*) forniti dalla stessa ai propri agenti di vendita al fine di migliorare la tempestività e l'accuratezza del sevizio di supporto alla clientela. Nel caso di specie, il Garante ha ritenuto conforme il trattamento ai principi in materia di protezione dei dati personali, subordinando la liceità dello stesso all'adozione da parte della società istante di specifiche misure tecniche e accorgimenti posti a tutela dei diritti degli interessati anche in relazione a quanto prescritto in un caso analogo con provvedimento 9 ottobre 2014, n. 448 (doc. web n. 3505371).

Con provvedimento 15 giugno 2017, n. 269 (doc. web n. 6697925) è stata invece esaminata una richiesta di verifica preliminare presentata da una società che opera nel settore delle spedizioni espresse, concernente il trattamento di dati personali connessi all'utilizzo di un dispositivo informatico multifunzione (denominato *mobile worker incab*) fornito ai corrieri della società, dotato della funzionalità GPS per la localizzazione di specifici eventi predeterminati e di un programma che consente di ottimizzare i processi di ritiro e consegna nonché gestione delle merci nel magazzino della filiale di riferimento.

Detto sistema (denominato *dynamic planning*), piuttosto complesso nella sua articolazione in quanto coinvolge informazioni relative ai corrieri e ai clienti (questi ultimi nella duplice veste di mittenti e di destinatari dei pacchi) nonché alle persone, diverse dai clienti, che effettivamente ricevono o consegnano la merce presso l'indirizzo dei clienti apponendo la propria sottoscrizione autografa sui documenti di trasporto, oltre a prevedere la digitalizzazione dei documenti di trasporto, consente l'aggiornamento in tempo reale dei dati relativi ai servizi affidati agli autisti, veicolando verso ciascuno soltanto i messaggi e le informazioni necessarie allo svolgimento della sua attività.

L'Autorità, anche a seguito delle modifiche che la società ha ritenuto di apportare al sistema *dynamic planning* sulla base di alcune criticità emerse nel corso dell'istruttoria, ha accolto, seppure con qualche limitazione, il progetto esaminato.

In particolare il Garante, dopo aver autorizzato il trattamento dei dati riferiti a tutti i soggetti interessati indipendentemente dal consenso degli stessi in applicazione della disciplina sul cd. bilanciamento di interessi (art. 24, comma 1, lett. *g*), del Codice), nell'escludere la possibilità di una rilevazione continuativa dei dati relativi alla localizzazione geografica degli interessati, ha individuato gli eventi al verificarsi dei quali la stessa è consentita e i tempi di conservazione delle diverse tipologie di dati in ragione delle finalità in concreto perseguite.

Particolari cautele sono state inoltre previste con riferimento all'accesso ai dati di localizzazione da parte delle diverse figure di utenti autorizzati (amministratore centrale del sistema, amministratore locale e utente operativo), nonché al fine di garantire l'integrità dei dati e prevenire l'accesso agli stessi da parte di soggetti non autorizzati.

In relazione ad un diverso ambito imprenditoriale, l'Autorità, con provvedimento 15 settembre 2017, n. 345 (doc. web n. 6826368) ha poi valutato positivamente un'istanza di verifica preliminare relativa al trattamento di dati personali connesso all'installazione di un'applicazione informatica che, nell'ambito dell'erogazione in diretta *streaming* di corsi di formazione professionale per avvocati, consente di verificare l'effettiva corrispondenza tra l'identità del professionista iscritto al corso e quella della persona connessa in diretta *streaming* (e quindi presente alla postazione informatica). Tale verifica, necessaria per l'attribuzione dei crediti formativi ai professionisti che abbiano effettivamente fruito della formazione a distanza (come previsto dal regolamento per la formazione professionale continua adottato il 16 luglio 2014 dal Consiglio nazionale forense), mira ad evitare che alcuni partecipanti pongano in essere comportamenti sleali, quali la sostituzione di persona.

Il Garante, avendo accertato, nel corso dell'istruttoria, che il predetto controllo – che si sostanzia in una operazione di confronto tra le immagini fotografiche dei partecipanti ai corsi quali risultano nei documenti di identità presentati al momento dell'iscrizione e quelle successivamente acquisite, ad intervalli regolari, via *webcam* – non comporta un trattamento di dati biometrici (per i quali sarebbe stata necessaria l'adozione di particolari cautele, cfr. provv. 12 novembre 2014, n. 513, doc. web n. 3556992), ha riconosciuto la liceità del trattamento in questione secondo le modalità illustrate dalla società. In particolare, fermo restando che il sistema informatico deve essere oggetto di una specifica e articolata informativa che, tra l'altro, descriva le caratteristiche tecniche del sistema ed evidenzi i tempi di conservazione dei dati, il Garante ha sottolineato come il sistema debba essere configurato in modo tale che i dati personali degli interessati (fotografie e diagrammi di connessione) siano trattati nel rispetto dei principi di proporzionalità e di necessità di cui agli artt. 3 e 11 del Codice.

Altro caso particolare esaminato dall'Autorità ha riguardato una richiesta di autorizzazione al trattamento di dati sensibili avanzata dal centro ricerche Fiat, società che promuove e realizza, in partenariato con diversi portatori di interesse pubblici e privati, numerosi progetti di ricerca e innovazione nel campo della mobilità sostenibile, in relazione ad un'attività di ricerca volta a migliorare la qualità e la sicurezza dei sistemi e dispositivi per i veicoli, attraverso la predisposizione di alcuni *test* e prove da sottoporre ad un campione di volontari che, previo consenso scritto, si renderanno disponibili ad eseguire le prove sperimentali utilizzando sia i veicoli sia i simulatori di guida.

Il progetto, promosso nell'ottica di favorire poi l'applicazione industriale dei risultati della ricerca in un'ottica di sostenibilità ambientale, economica e sociale, consisterebbe nell'acquisizione di informazioni connesse alle condizioni fisiche ed alle reazioni comportamentali dei soggetti coinvolti nelle sperimentazioni, anche attraverso la raccolta di informazioni sensibili quali quelle relative alla frequenza cardiaca, all'attività muscolare, all'attività elettrica dell'encefalo, nonché alla conduttanza cutanea.

Nell'ambito dell'istruttoria è stato specificato che le misure di sicurezza adottate a tutela del trattamento dei dati personali e sensibili saranno caratterizzate da una procedura specifica di separazione tra i dati sensibili memorizzati nel corso della prova e l'identità del soggetto da cui i dati stessi provengono.

Con provvedimento 5 ottobre 2017, n. 392 (doc. web n. 7297741) il Garante ha autorizzato il descritto trattamento di dati personali sensibili limitatamente alle informazioni indispensabili per l'elaborazione dei risultati dei *test* di "usabilità", di simulazione di guida e di conduzione di veicolo.

14.6. *Indagine conoscitiva sui* big data

Nel corso dell'anno, sulla base di un'iniziativa avviata il 30 maggio 2017 unitamente all'Autorità garante della concorrenza e del mercato e all'Autorità per le garanzie nelle comunicazioni, l'Autorità è stata impegnata in un ciclo di audizioni con esperti e imprese operanti in vari settori dell'economia (OTT e società che si occupano di *data analytics* e *data trading*, editori e imprese del settore audiovisivo e media, imprese del mondo assicurativo e bancario) sulla tematica dei *big data*. Si tratta di un'indagine conoscitiva ancora in corso, finalizzata ad individuare eventuali criticità connesse ai *big data* e a definire, se del caso, un quadro di regole atto a promuovere la concorrenza dei mercati nell'economia digitale, la protezione dei dati personali e i diritti del consumatore, nonché i diversi profili del pluralismo nell'ecosistema digitale.

15 L'attività di normazione tecnica internazionale e nazionale

Nel 2017 l'Autorità ha proseguito la collaborazione in tema di elaborazione di norme tecniche internazionali nell'ambito del *Working group* 5 del sottocomitato SC27, che si occupa della sicurezza delle informazioni all'interno del comitato tecnico JTC1 dell'organizzazione internazionale per la normazione (ISO). Il gruppo di lavoro segue gli aspetti di sicurezza nella gestione delle identità relativamente alla tecnologie biometriche e alla protezione dei dati personali.

Il Garante, armonizzando la propria posizione con quelle delle altre autorità di protezione dei dati tramite il WP Art. 29, che ha una *liason* in proposito con ISO, ha seguito lo sviluppo delle norme tecniche di seguito riportate:

– ISO 20889 - *Privacy enhancing data de-identification techniques*: *standard* che fornisce una descrizione delle tecniche di de-identificazione utili nella progettazione di misure atte a rafforzare la *privacy* in accordo con i princìpi previsti dalla norma ISO/IEC 29100 *privacy framework*;

– ISO 29184 - *Guidelines for online privacy notice and consent*, che definisce una serie di requisiti per fornire l'informativa e acquisire il consenso *online* in modalità *user friendly*;

– ISO 27552 - *Information technology - Security techniques – Enhancement to* ISO/IEC *27001 for privacy management – Requirements*, che stabilisce i requisiti di un sistema di gestione della *privacy* delle informazioni (PIMS) a completamento di un sistema di gestione per la sicurezza delle informazioni (ISMS - ISO 27001).

L'Autorità ha altresì proseguito la collaborazione con UNINFO, l'ente di normazione federato con UNI (Ente nazionale italiano di unificazione), contribuendo alle seguenti attività:

– stesura della norma tecnica UNI 11697:2017 – Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza che, a partire dalla metodologia per la costruzione di profili professionali basati sul sistema e-CF (norme UNI 11506 e UNI 11621-1), che individua i profili e le competenze dei professionisti che lavorano in ambiti connessi al trattamento e alla protezione dei dati personali;

– stesura di un rapporto tecnico sui criteri d'identificazione delle *app* nel settore socio-sanitario per una corretta caratterizzazione delle *app* nonché maggiore consapevolezza degli utilizzatori.

16 Il trattamento dei dati personali nell'ambito del condominio

Tra le questioni affrontate dall'Autorità sul tema del trattamento di dati personali in ambito condominiale di particolare interesse è stato il quesito relativo alla corretta interpretazione della disposizione introdotta dalla legge n. 220/2012 (cd. riforma del condominio) e contenuta nell'art. 63, comma 5, disp. att. c.c. (ciò anche in relazione a quanto previsto nell'art. 1130, comma 1, n. 6, c.c.).

In particolare, si è chiesto al Garante di pronunciarsi in ordine alla possibilità che la copia autentica del titolo che determina il trasferimento del diritto di proprietà di un immobile (che in base alla norma citata deve essere oggetto di trasmissione all'amministratore di condominio da parte di "chi cede diritti su unità immobiliari") possa essere rilasciata dal Pubblico Ufficiale con "*omissis*", anziché nella forma della copia autentica. Ciò al fine di limitare la quantità di dati personali non pertinenti portati a conoscenza di soggetti estranei alla compravendita immobiliare. Nell'ottica di fornire un'interpretazione in ordine alla corretta applicazione della norma, il Garante, in ragione delle peculiari questioni di natura civilistica sottese al quesito proposto, ha ritenuto opportuno consultare il Consiglio nazionale del notariato (Cnn) che, nel confermare quanto già rappresentato in un precedente studio condotto sul tema (cfr. studio del 23 maggio 2013, n. 320-2013/C su "La riforma del condominio – Prime riflessioni su alcune delle nuove disposizioni di interesse notarile"), ha ribadito che la finalità informativa cui la norma è preordinata deve ritenersi soddisfatta anche con la "dichiarazione di avvenuta stipula" rilasciata dal notaio rogante.

All'esito degli articolati approfondimenti condotti sul tema e in considerazione di quanto emerso nel confronto con il Cnn, il Garante ha quindi concluso che la modalità sopra indicata – che può dunque considerarsi equipollente in termini di autenticità e certezza a quella prevista dal legislatore – rappresenta una valida alternativa, conforme ai principi in materia di protezione dei dati personali di cui all'art. 11, comma 1, lett. *d*), del Codice, alla trasmissione della copia autentica dell'atto che determina il trasferimento da parte dell'interessato. Il condomino interessato sarà pertanto legittimato a chiedere al notaio rogante tale dichiarazione, purché la stessa sia provvista di tutte le indicazioni utili all'amministratore ai fini della tenuta del registro dell'anagrafe condominiale (v. *newsletter* 30 ottobre 2017, n. 434, doc. web n. 7054700).

17 Il trasferimento dei dati personali all'estero

Con riferimento ai flussi transfrontalieri di dati personali, l'attività del Garante si è caratterizzata prevalentemente sul piano delle autorizzazioni ai trasferimenti di dati personali verso Paesi terzi mediante regole vincolanti d'impresa (*Binding corporate rules* – Bcr) e si è conclusa, al termine di complesse istruttorie, con l'approvazione di 13 provvedimenti autorizzatori.

Tale attività, alla stregua delle verifiche poste in essere negli anni precedenti in relazione ad analoghe istanze, ha interessato la conformità con l'ordinamento italiano del testo delle Bcr approvato al termine della procedura europea di cooperazione al fine di verificare la rispondenza, anche sul piano fattuale, degli impegni assunti dalle società istanti rispetto ai criteri stabiliti al riguardo dal Gruppo Art. 29; nell'ambito di alcuni procedimenti sono state acquisite maggiori informazioni nonché, ove necessario, idonee rassicurazioni, soprattutto in materia di clausola del terzo beneficiario, regime di responsabilità, natura e finalità delle operazioni di trasferimento poste in essere (cfr. provv.ti 16 gennaio 2017, n. 61, doc. web n. 6186347; 26 gennaio 2017, n. 27, doc. web n. 6068057; 9 marzo 2017, n. 129, doc. web n. 6341672; 23 marzo 2017, n. 151, 6343033; 30 marzo 2017, n. 166, doc. web n. 6388305; 18 maggio 2017, n. 237, doc. web n. 6531046; 5 luglio 2017, n. 305, doc. web n. 6826765; 20 luglio 2017, n. 325, doc. web n. 6819647; 5 ottobre 2017, n. 407, doc. web n 7274188; 30 novembre 2017, n. 504, doc. web n. 7457490; 21 dicembre 2017, n. 552, doc. web n. 7563753).

In altri casi, le istanze di autorizzazione pervenute hanno avuto ad oggetto Bcr già precedentemente autorizzate dal Garante e provenienti da società di gruppo intenzionate ad aderire alle suddette Bcr in epoca successiva all'emanazione dei citati provvedimenti di autorizzazione: in queste ipotesi, le relative autorizzazioni sono state rilasciate, mediante estensione a tali procedimenti, previa espressa conferma in tal senso resa dalle società istanti, delle informazioni e chiarimenti già acquisiti in precedenza dall'Autorità (cfr. provv.ti 12 gennaio 2017, n. 3, doc. web n. 6033601; 15 giugno 2017, n. 270, doc. web n. 6630481).

18 Il registro dei trattamenti

18.1. *La notificazione*

La notificazione è una dichiarazione con la quale il titolare del trattamento (sia 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).

È importante tenere sempre in considerazione che 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.

Sui titolari che hanno notificato un trattamento incombe l'onere di mantenere aggiornato il registro comunicando le eventuali variazioni (ad es., 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, e 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 i provvedimenti di esonero dall'obbligo di notificazione o di chiarimento adottati dal Garante che sono tutti pubblicati, insieme alle istruzioni, nella sezione del sito istituzionale denominata "Notificazione e Registro dei trattamenti", raggiungibile dalla *home page* cliccando il *link* servizi *online*.

18.2. *L'evoluzione delle notificazioni nel 2017*

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 trattamenti che necessitano di essere notificati.

Nel 2017 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 nell'anno sono emersi n. 33 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).

In tutti i casi in cui sono state riscontrate violazioni 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 riscontrate e contestate ai titolari e del conseguente adempimento da parte degli stessi e degli altri operatori del settore, nel 2017 sono confluite nel Registro dei trattamenti n. 3.179 nuove notificazioni, a fronte di 2.369 notificazioni nel 2016 e di una media inferiore a n. 1.600 notificazioni annue negli ultimi dodici anni.

La pubblicazione di un gruppo di risposte alle domande più frequenti (cd. FAQ) sul sito istituzionale, realizzata al fine di agevolare la comunicazione verso l'utenza su aspetti, sia di natura tecnica che di merito, legati alla procedura di notificazione, ha consentito di far fronte in maniera efficace alla rinnovata attenzione per tale adempimento normativo. Nel 2017, a fronte del notevole incremento del numero di notificazioni effettuate, l'aumento delle richieste di informazioni rispetto all'anno precedente è stato, sensibilmente inferiore. Sono pervenute circa 1.000 richieste di chiarimento telefoniche (800 nel 2016) e circa 350 tramite posta elettronica (250 nel 2016), a cui è stato fornito un tempestivo riscontro.

19 La trattazione dei ricorsi

19.1. *I profili generali*

L'art. 77 del RGPD stabilisce che "Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo ad un'autorità di controllo […]". La lettera della disposizione consentirebbe quindi di mantenere in vita la procedura dei ricorsi sin qui prevista dagli artt. 145 ss. del Codice. Esigenze di coordinamento con le altre autorità di protezione dati stabilite dalle procedure di cooperazione e di coerenza introdotte dal RGPD fanno però ritenere che tale specifico procedimento cesserà con l'entrata in vigore del nuovo quadro normativo e che tutte le doglianze degli interessati saranno esaminate nell'ambito della procedura dei "reclami", uniforme per tutti i Paesi dell'Unione europea.

L'istituto del ricorso, tuttavia, lascia un'importante esperienza nel nostro Paese che l'Autorità cercherà di non disperdere sia sotto il profilo procedurale che sotto quello del *modus operandi*, improntato a principi di effettività, deburocratizzazione e accesso facilitato agli interessati/ricorrenti.

Volendo dar conto di quanto avvenuto nell'anno 2017, può essere utile un primo sguardo di insieme ai dati statistici ed un loro rapido confronto con quelli dell'anno precedente.

Anche per l'anno in corso, il primo elemento che viene in evidenza è la sostanziale conferma del consolidamento che si registra in determinati settori oggetto di ricorso, i quali, dopo periodi di notevole impatto, anche numerico, via via che si delineano i confini delle pretese, si riducono sino a diventare del tutto marginali. È il caso, ad esempio, dei ricorsi relativi ai Sistemi di informazioni creditizie (Sic) fermo al 4% nel 2016 e che si riduce ulteriormente al 3% nel 2017.

Rimane sostanzialmente stabile (29% rispetto al 31%) la percentuale dei ricorsi presentati nei confronti degli editori, all'interno dei quali un ruolo assolutamente preponderante è ricoperto da quelli diretti a testate giornalistiche o a motori di ricerca per il riconoscimento – in forma più o meno corretta, come si vedrà – del cd. diritto all'oblio.

Si può quindi parlare di un *trend* stabile, di valore relativo senz'altro rilevante (quasi un terzo dei ricorsi presentati), legato da un lato alle nuove opportunità offerte dalla sentenza della Corte di giustizia dell'Unione europea 13 maggio 2014 C-131/12 (sentenza Google Spain), ma che, come si segnalava nella precedente Relazione, probabilmente, costituisce anche la spia di un'aumentata percezione degli effetti negativi che la permanenza sul web di notizie risalenti nel tempo, spesso parziali o superate da eventi successivi, può comportare sulla sfera personale dell'individuo e nelle sue relazioni con il mondo esterno. Nell'anno in considerazione, infatti, si registra all'interno dei numeri sopra evidenziati un aumento di interventi con riguardo a notizie non aggiornate per le quali il ricorso ai "siti fonte" si sarebbe rivelato particolarmente complesso.

In questo senso, come si vedrà nell'illustrazione di alcuni tra i casi affrontati dal Garante, si rende necessario delimitare con attenzione l'ambito di applicazione di tale diritto, tenendo conto certamente delle aspirazioni dell'interessato, ma anche

del generale diritto della collettività ad essere informata ed alla conservazione della memoria storica.

Così come occorre tenere ben distinto il diritto all'oblio da altri aspetti, quali ad esempio quelli legati ad interventi di carattere diffamatorio che, lanciati sul web, vedono aumentata la loro portata pregiudizievole, ma che – salvo rari casi – non possono essere esaminati nell'ambito del sistema di tutela approntato dal Codice.

Sempre in via generale, l'esame dei dati complessivi sotto il profilo numerico mantiene il livello dell'anno precedente (276 nel 2017 e 277 nel 2016), confermando il decremento di circa il 9% rispetto al 2015 (307 ricorsi).

19.2. *I dati statistici*

Scendendo ad un maggior grado di dettaglio nell'esame dei dati statistici riferiti all'anno 2017 e prestando attenzione sia alla tipologia di decisioni adottate, sia alle categorie di titolari del trattamento, emergono ulteriori informazioni che può essere utile evidenziare.

Per ciò che concerne la tipologia delle decisioni si conferma, in modo del tutto evidente, l'alto numero di provvedimenti di non luogo a provvedere (53% del totale), cioè di procedimenti conclusisi con il soddisfacimento, nel corso dell'istruttoria, delle richieste dei ricorrenti. Una percentuale così alta depone senz'altro a favore dell'utilità e dell'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 previsti e 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.

Si mantiene stabile anche la percentuale delle decisioni di inammissibilità pari al 17% (18% nel 2016) da leggersi in parte con riferimento a situazioni contingenti ed in parte in un'ottica di maggior valorizzazione di alcuni profili procedurali, necessaria nell'evoluzione di uno strumento di tutela che ormai può essere considerato come "maturo" e nella conseguente prospettiva di passaggio dettata dal nuovo regolamento.

Non meno significativo è lo sguardo alle principali categorie di titolari del trattamento, sia pubblici che privati, dove si nota immediatamente il dimezzamento dei ricorsi presentati nel settore bancario e delle società finanziarie, che passa dal 26% dei casi complessivi nel 2016 al 12%, indicatore di una sempre più elevata consapevolezza dei titolari rispetto alle richieste rivolte dagli interessati.

A seguire, si rileva anche nell'anno in considerazione un numero relativamente alto di procedimenti attivati nei confronti dei datori di lavoro pubblici e privati (11% nel 2017 contro il 12% nel 2016), spesso legati a situazioni conflittuali tra datori di lavoro e lavoratori e, in particolare, a procedure di contestazione disciplinare o di licenziamento. Rilevante in tale settore è il numero di ricorsi aventi ad oggetto il corretto uso degli strumenti informatici aziendali messi a disposizione del lavoratore.

Può destare qualche sorpresa il sensibile incremento dei ricorsi presentati nei confronti delle amministrazioni pubbliche e dei concessionari di pubblici servizi (44, nel 2017, contro i 12 del 2016 e i 20 del 2015), ma su questi incide sensibilmente la presentazione di 28 ricorsi proposti dai dirigenti di un'unica amministrazione per la medesima questione. Depurati di tale specificità il numero si colloca nella media dei due anni precedenti.

Cresce invece il numero dei ricorsi relativi all'attività di *marketing* svolta da

imprenditori privati, che dal 3% del 2016 si colloca al 7% del totale nel 2017, nonché all'attività dei fornitori telefonici e telematici (anche qui passando dal 3 al 6%), ritornando in entrambi i casi ai livelli del 2015.

Non superano, poi, il 5% i ricorsi diretti verso altre singole categorie di titolari: strutture sanitarie pubbliche e private (che passano però dal 2 al 5%); liberi professionisti (2%); centrale rischi Banca d'Italia (1%); associazioni e amministrazioni condominiali (entrambe all'1%).

Infine, si assottiglia ulteriormente la restante quota dei ricorsi rivolta contro altri titolari – che singolarmente non superano la soglia dell'1% – che passa dal 4% complessivo del 2016 al 2% del 2017.

19.3. *La casistica più significativa*

Tra i casi più significativi presi in esame dal Garante nel periodo in considerazione, possono elencarsi i seguenti, suddivisi per ambito tematico di riferimento.

Trattamenti in ambito giornalistico

In ambito giornalistico, come accennato, il 2017 è stato caratterizzato da un elevato numero di ricorsi, molti di questi incentrati sul rispetto del cd. diritto all'oblio.

I principi già enucleati dall'Autorità e delineati in forma sistematica dalla sentenza Google Spain e dalla successiva attività interpretativa realizzata dal Gruppo Art. 29, hanno dovuto trovare pratica applicazione nella varia casistica portata all'attenzione del Garante nel corso dell'anno.

Tra i casi più importanti, anche sotto il profilo procedurale, va menzionata la decisione assunta dal Garante il 9 novembre 2017, n. 470 (doc. web n. 7465698) riguardante la richiesta di rimozione rivolta a tre distinti motori di ricerca (Google, Yahoo! e Bing) di un URL che, mediante digitazione del nominativo dell'interessato, rinviava ad una vicenda giudiziaria in cui questi era rimasto coinvolto nel 2007, conclusasi con l'applicazione di pena su richiesta delle parti e con il beneficio della sospensione condizionale. Nel corso del procedimento Yahoo! Emea Ltd. e Yahoo! Italia s.r.l., pur fornendo i riscontri richiesti hanno eccepito la carenza di giurisdizione del Garante; lo stesso hanno fatto Microsoft Corp. e Microsoft s.r.l. (quest'ultima rilevando peraltro il difetto di legittimazione passiva, sostenendo che la società che gestisce il motore di ricerca Bing fosse solo Microsoft Corp.). Il Garante, in via preliminare, ha confermato la propria competenza nei confronti di tutte le resistenti ribadendo quanto già disposto in precedenti decisioni (cfr. provv.ti 25 febbraio 2016, n. 83, doc. web n. 4881581; e 26 gennaio 2017, n. 30, doc. web n. 6026501) e tenendo a mente anche le disposizioni di cui agli artt. 3 e 77 del RGPD. Nel merito, considerato che i fatti narrati nell'articolo in questione risalivano a circa dieci anni orsono e che l'universalità della diffusione e dell'accessibilità delle informazioni ivi contenute comportava un impatto sproporzionatamente negativo nella sfera di riservatezza dell'interessato, sono state riconosciute le ragioni del ricorrente ritenendo illecito il trattamento in questione.

Un'importante precisazione è stata poi fornita dall'Autorità con la decisione del 15 giugno 2017, n. 277 (doc. web n. 6692214) chiarendo che la citata sentenza della Corte di giustizia, secondo la quale la ricerca può essere effettuata a partire "dal nome", non esclude la possibilità che a questo possano essere associati ulteriori termini diretti a specificarla: in particolare, nel caso di specie, si chiedeva la rimozione di URL ai quali si giungeva partendo dal nome e dal cognome dell'interessato in aggiunta ad ulteriori informazioni legate alla sua vita professionale.

Ulteriore precisazione di rilievo in tale materia si è avuta anche con la decisione del 21 dicembre 2017, n. 557 (doc. web n. 7465315) che è intervenuta sulla possi-

bilità o meno di estendere eventuali decisioni di deindicizzazione anche sulle versioni extra-UE del motore di ricerca, questione portata all'attenzione della Corte di giustizia con rinvio pregiudiziale da parte del Consiglio di Stato francese. Nel caso considerato – nel quale il ricorrente aveva dichiarato di risiedere e di svolgere la propria attività lavorativa prevalentemente al di fuori dell'Unione europea –, l'Autorità ha ritenuto che la richiesta di rimozione di alcuni URL dovesse essere estesa a tutti i risultati di ricerca, sia nelle versioni europee che extra-europee del motore, al fine di assicurare l'effettività della tutela dell'interessato.

Accanto alla tipologia che ormai possiamo definire "classica" di applicazione del diritto all'oblio, diverse decisioni sono andate a disciplinare particolari applicazioni del rapporto tra notizia originaria e successivo trattamento da parte del motore di ricerca.

Così, con provvedimento 13 aprile 2017, n. 191 (doc. web n. 6548076), l'Autorità ha accolto le ragioni del ricorrente ritenendo illecito il trattamento operato da Google relativamente ad un articolo di stampa che riportava, con dovizia di particolari (comprese analitiche informazioni sulla salute), la notizia di un trattamento sanitario obbligatorio subito dall'interessato alcuni anni prima, tanto da configurare già *ab origine* un trattamento in contrasto con i principi fissati dal codice deontologico per la professione giornalistica. La mancanza di informazioni integrative sulla vicenda processuale privava poi l'originaria notizia dei necessari requisiti di esattezza ed aggiornamento con contestuale violazione dell'art. 11 del Codice.

Sempre dando rilievo ai principi posti dall'art. 6 della direttiva e dell'art. 11 del Codice è stato poi accolto il ricorso di una persona (provv. 6 aprile 2017, n. 181, doc. web n. 6517133) avente ad oggetto la richiesta volta ad ottenere la rimozione di ventisette URL che rinviavano ad articoli riferiti ad una vicenda giudiziaria nella quale l'interessato era rimasto coinvolto, ma che risultavano non aggiornati alla luce dei successivi sviluppi della stessa, conclusasi con una sentenza di patteggiamento con concessione del beneficio di sospensione della pena e non menzione nel casellario giudiziale.

La richiesta di deindicizzazione rivolta al motore di ricerca ha mostrato la sua utilità anche in alcuni casi particolari in cui sarebbe risultato eccessivamente complicato, se non impossibile, ottenere soddisfazione dai gestori dei "siti fonte". È il caso del provvedimento adottato il 9 marzo 2017, n. 132 (doc. web n. 6431003) in merito alla richiesta di rimozione di tre URL che rinviavano ad un *post* anonimo, pubblicato su alcuni siti extra-europei, ritenuto lesivo dall'interessato. L'Autorità ha accolto il ricorso rilevando che le notizie in questione, oltre che risalenti nel tempo, non erano state confermate da altri interventi, né da ulteriori elementi di carattere oggettivo: inoltre, il *post* risultava essere anonimo o, comunque, non riportava alcuna indicazione utile che consentisse di identificare l'autore al quale poter rivolgere direttamente eventuali istanze ai sensi del Codice.

In senso analogo è stato deciso un ulteriore ricorso (provv. 26 gennaio 2017, n. 30, doc. web n. 6026501) che traeva origine dalla richiesta dell'interessato volta ad ottenere la rimozione di alcuni URL che rinviavano ad informazioni attinenti una vicenda nella quale lo stesso era stato coinvolto, pubblicate all'interno di un sito statunitense.

Trattamenti in ambito lavorativo

Fra i trattamenti effettuati da parte di datori di lavoro, l'Autorità è nuovamente intervenuta in materia di corretto utilizzo degli strumenti di posta elettronica aziendale, venendo chiamata spesso a valutare i delicati rapporti derivanti dall'utilizzo di tali strumenti a fini disciplinari o anche di risoluzione del rapporto.

Così, in particolare nel provvedimento del 13 settembre 2017, n. 375 (doc. web n. 7316160), esaminando la doglianza con cui l'interessato lamentava un trattamen-

to illecito dei dati contenuti nella propria posta elettronica da parte del datore di lavoro che li aveva poi utilizzati ai fini della contestazione disciplinare e del successivo licenziamento, ha rilevato un'effettiva inosservanza da parte di quest'ultimo degli artt. 11 e 13 del Codice, nonché delle indicazioni contenute nelle linee guida dettate dal Garante in materia di posta elettronica ed internet (doc. web n. 1387522). Il Garante ha quindi parzialmente accolto il ricorso vietando ogni ulteriore utilizzo dei dati illecitamente trattati, fatta salva la sola conservazione degli stessi ai fini dell'eventuale acquisizione da parte dell'autorità giudiziaria, ordinando alla resistente di consentire all'interessato di accedere alle informazioni personali richieste (in particolare, fotografie e codici personali). La comunicazione di queste ultime, in virtù della loro attinenza alla sfera privata del ricorrente, non è stata infatti giudicata idonea a pregiudicare le esigenze difensive del datore di lavoro nell'ambito dei giudizi pendenti tra le parti e ciò nonostante l'eccezione di differimento sollevata da quest'ultimo ai sensi dell'art. 8, comma 2, lett. *e*), del Codice.

In senso opposto è stata invece decisa un'ulteriore controversia (provv. 5 ottobre 2017, n. 403, doc. web n. 7429031) concernente la richiesta – avanzata da un ex dipendente alla società presso la quale prestava la propria attività – di accedere a tutte le comunicazioni di posta elettronica di carattere personale, inviate e ricevute durante l'intero corso di svolgimento del rapporto di lavoro, contenute all'interno degli strumenti aziendali utilizzati dal medesimo.

L'Autorità, aderendo all'eccezione di differimento sollevata dalla resistente ai sensi dell'art. 8, comma 2, lett. *e*), del Codice, ha rigettato il ricorso ritenendo sussistenti le rappresentate ragioni di potenziale pregiudizio derivanti dal disvelamento del contenuto di quanto domandato in considerazione della pendenza di un giudizio tra le parti innanzi al giudice del lavoro. Ciò tenuto conto, in particolare, del fatto che le comunicazioni presenti all'interno di un *account* di posta elettronica aziendale, pur potendo risultare apparentemente riconducibili a contenuti di natura personale, possono in realtà celare informazioni rilevanti ai fini della dimostrazione in giudizio delle condotte illecite addebitate al dipendente.

I casi sottoposti all'esame dell'Autorità hanno riguardato anche l'ambito del lavoro pubblico. Ad esempio, sono state portate all'attenzione del Garante da parte di un pubblico dipendente l'opposizione e la richiesta di blocco del trattamento dei propri dati personali contenuti in alcune sue comunicazioni di posta elettronica utilizzate dal datore di lavoro nell'ambito di un procedimento disciplinare. In particolare, quest'ultimo lamentava l'illiceità del trattamento di propri dati personali comuni e sensibili, derivante dalla violazione dell'art. 11 del Codice, nonché degli artt. 1 e 8, l. n. 300/1970, consistente nell'indebito utilizzo a fini disciplinari di opinioni personali aventi peraltro rilievo sindacale. All'esito dell'istruttoria è emerso che il trattamento posto in essere dal datore di lavoro era stato effettuato nell'ambito del legittimo esercizio del potere disciplinare ad esso spettante. L'Autorità ha pertanto dichiarato il ricorso infondato (provv. 20 aprile 2017, n. 202, doc. web n. 6552839).

Trasparenza

Sempre nell'ambito del rapporto di lavoro pubblico sono stati presentati all'Autorità 28 ricorsi da parte di altrettanti dirigenti di una azienda sanitaria (27 dei quali però giudicati inammissibili per assenza di un trattamento in atto al momento della loro presentazione) aventi ad oggetto l'opposizione al trattamento, mediante diffusione sul sito dell'azienda sanitaria, dei dati patrimoniali in attuazione degli obblighi di pubblicazione di cui al decreto legislativo 14 marzo 2014, n. 33, nel testo novellato dal decreto legislativo 25 maggio 2016, n. 97. Il ricorrente, direttore di un Dipartimento dell'azienda, ha contestato l'applicabilità della disposizione che impone l'obbligo di pubblicazione dei dati patrimoniali dei dirigenti e ciò in virtù

del regime differenziato previsto dalla normativa sulla trasparenza con riguardo alla dirigenza del Servizio sanitario nazionale. Il Garante, ritenendo condivisibile l'interpretazione prospettata dall'interessato, ha accolto il ricorso ordinando al titolare del trattamento di astenersi dalla diffusione dei dati in tal modo raccolti che, in assenza di una disposizione normativa di carattere autorizzativo, darebbe luogo ad un trattamento illecito ai sensi dell'art. 19, comma 3, del Codice (provv. 30 marzo 2017, n. 175, doc. web n. 6260581).

Benché ormai molto ridotti nel numero, alcuni ricorsi presentati nell'ambito dei Sic hanno consentito di risolvere nuovi dubbi interpretativi. Nel corso dell'anno (provv. 19 ottobre 2017, n. 430, doc. web n. 7441510) è stata esaminata, ad esempio, la richiesta di cancellazione di due segnalazioni "a sofferenza" inserite da un istituto bancario nel sistema di informazioni creditizie gestito da Crif s.p.a., in relazione ad inadempimenti, non successivamente regolarizzati ed ancora presenti nella banca dati nonostante il titolare del trattamento avesse deciso l'estinzione dei rapporti già nel marzo 2013. Il Garante ha accolto il ricorso, in ragione del fatto che l'art. 6, comma 5, del codice deontologico di settore fissa in 36 mesi il tempo di conservazione nei Sic delle informazioni di tipo negativo riguardanti inadempimenti non successivamente regolarizzati e stabilendo, tra i casi nei quali tale termine inizia a decorrere, anche "la data di cessazione del rapporto". Si è, a tal riguardo, ritenuto che la risoluzione del contratto da parte della banca concretizzi motivo di "cessazione del rapporto", momento dal quale, dunque, far decorrere il computo dei termini di conservazione in base al codice deontologico di settore.

Tale interpretazione è stata poi ripresa nel "provvedimento interpretativo di alcune disposizioni del codice Sic", adottato dal Garante il 26 ottobre 2017, n. 438 (doc. web n. 7221677).

20 Il contenzioso giurisdizionale

20.1. *Considerazioni generali*

Come riferito nelle precedenti Relazioni, l'art. 34, d.lgs. n. 150/2011 ha abrogato l'art. 152 del Codice, con l'eccezione del comma 1, dettando all'art. 10 regole procedurali concernenti le controversie in materia di applicazione delle disposizioni del Codice. In particolare, l'art. 34 ha abrogato anche 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 effettuate al Garante che, in alcuni casi, l'autorità giudiziaria ha continuato a ritenere necessaria; a fronte dei 19 ricorsi notificati nel 2015 e dei 12 nel 2016, nel 2017 sono stati notificati all'Autorità e da questa trattati 14 ricorsi.

Attesa l'importanza di tale strumento posto a disposizione degli interessati e volto alla tutela giurisdizionale del diritto alla protezione dei dati personali in alternativa al ricorso presentato in sede amministrativa al Garante, assume quindi 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 misura, unitamente alle notifiche dei ricorsi proposti direttamente davanti al giudice che l'autorità giudiziaria riterrà di effettuare, potrà consentire al Garante di continuare ad avere più facilmente conoscenza dell'evoluzione della giurisprudenza in materia di protezione dei dati personali e di svolgere il ruolo di segnalazione 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).

Si consideri peraltro che in base all'art. 58, par. 5, RGPD, "Ogni Stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso", e similmente l'art. 47, par. 5, della direttiva 680/2016, prevede che "Ogni Stato membro dispone per legge che ciascuna autorità di controllo abbia il potere di sottoporre all'attenzione di autorità giudiziarie violazioni delle disposizioni adottate a norma della presente direttiva e, se del caso, di intentare un'azione o di agire in sede giudiziale, per far rispettare le disposizioni adottate a norma della presente direttiva".

20.2. *I profili procedurali*

In tema di incompetenza funzionale, la Corte di appello di Lecce, con sentenza 23 maggio 2017, n. 555, decidendo sull'impugnazione di una sentenza del Tribunale di Lecce in materia di invio di fax di carattere commerciale in assenza di consenso, ha dichiarato l'inammissibilità dell'appello, in quanto ai sensi dell'art.

152, comma 13, del Codice, avverso la sentenza si sarebbe dovuto proporre ricorso direttamente dinanzi alla Corte di cassazione (23 maggio 2017, n. 555).

In altri due casi, la Corte di cassazione, confermando quanto statuito dal Tribunale di Vibo Valentia, che si era dichiarato incompetente (v. Relazione 2016, p. 130), e del Tribunale di Napoli, ha disposto che il foro speciale del consumatore di cui all'art. 33, comma 2, lett. *u*), d.lgs. 6 settembre 2005, n. 206, prevale sul foro del titolare del trattamento, previsto in via generale dall'art. 10, d.lgs. n. 150/2011, in ragione delle esigenze di tutela del consumatore in sede processuale, solo se il trattamento si inserisce in modo qualificato all'interno del rapporto di consumo (7 marzo 2017, n. 5658; 17 maggio 2017, n. 954).

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

20.3. *Le opposizioni ai provvedimenti del Garante*

L'anno 2017 ha registrato un leggero decremento nella proposizione delle opposizioni a provvedimenti dell'Autorità, 73, a fronte degli 80 ricorsi del 2016. Di queste, 38 si riferiscono a opposizioni a ordinanze ingiunzioni, in aumento rispetto al 2016 (35).

Di seguito si dà conto delle sentenze di maggior rilievo.

Opposizioni a ordinanze ingiunzioni

Nel periodo di riferimento sono state effettuate 55 opposizioni a provvedimenti del Garante (delle quali 38 hanno avuto ad oggetto ordinanze ingiunzioni) nei cui giudizi l'Autorità si è sempre costituita tramite l'Avvocatura dello Stato territorialmente competente.

Informativa e consenso

Tra le opposizioni alle ordinanze ingiunzioni, tre decisioni hanno riguardato l'omesso consenso; nelle prime due, il consenso risultava già preselezionato e non poteva considerarsi sussistente un'inequivoca manifestazione di volontà dell'interessato; pertanto le pronunce, avvalorando la giurisprudenza costante, hanno confermato le valutazioni dell'Autorità espresse nei provvedimenti, rispettivamente, del 18 dicembre 2014, nn. 612 (doc. web n. 3745935) e 613 (doc. web n. 3750400) e rigettato i ricorsi (Trib. Roma, 21 aprile 2017, n. 7400 e 19 settembre 2017, n. 17591). Nell'ultimo caso, oggetto del provvedimento del Garante 16 aprile 2015, n. 228 (doc. web n. 4205347), il Tribunale di Trento non ha valutato sufficiente un unico consenso per cinque distinti *form* di raccolta dati su un sito web, ritenendo invece necessario uno specifico consenso per ogni finalità del trattamento (22 maggio 2017, n. 1187).

Un'altra pronuncia ha avuto ad oggetto la cessione di un *database* contenente oltre duecentomila utenze telefoniche utilizzate per l'invio di sms di propaganda elettorale da una società ad un'altra senza informativa né consenso.

La Corte di cassazione (3 maggio 2017, n. 18619), annullando con rinvio la sentenza del Tribunale di Milano che aveva ridotto la sanzione ritenendo la violazione di modesta gravità in assenza di prove circa l'effettivo numero di utenti raggiunti da sms elettorali ed escludendo quindi l'applicazione dell'aggravante ai sensi dell'art. 164-*bis* del Codice, ha ritenuto – confermando il provvedimento del Garante del 13 giugno 2013, n. 291 (doc. web n. 2616804) – che occorreva guardare al numero dei soggetti interessati dal trasferimento dei dati e dal loro trattamento, essendo irrilevante se e quanti siano stati effettivamente raggiunti dai suddetti sms.

Quattro sentenze hanno riguardato l'attivazione di una pluralità di schede telefoniche effettuate da distinte società nei confronti di singoli interessati senza aver reso loro l'informativa.

20

In tutti i casi il giudice ha confermato il provvedimento del Garante, rispettivamente del 18 aprile 2013, n. 204 (doc. web n. 2691090); 1° aprile 2013, n. 189 (doc. web n. 2601680); 13 maggio 2015, n. 293 (doc. web n. 4210697) e 11 aprile 2013 n. 186 (doc. web n. 2575298): nei primi due casi ha ritenuto la circostanza provata sulla base degli elementi raccolti durante le indagini penali, mentre nell'ultimo caso la sanzione è stata rideterminata riducendola, in quanto il giudice non ha ritenuto applicabile il cumulo giuridico delle sanzioni con riferimento ad un'unica violazione di legge (Trib. Vicenza, 8 novembre 2016, n. 2554 e 28 febbraio 2017, n. 1040; Trib. Milano, 2 dicembre 2016, n. 12576 e Trib. Verona, 16 febbraio 2017, n. 409).

Una decisione ha confermato il provvedimento del Garante 20 giugno 2013, n. 303 (doc. web n. 2618747), con il quale era stata sanzionata una società che raccoglieva dati personali di natura anche sensibile di persone che dovevano sottoporsi a cicli di cure termali, poi trasmessi ad un'associazione per le valutazioni sanitarie, in assenza di consenso e informativa (Trib. Napoli, 5 ottobre 2015, n. 12598).

In altro caso, il Tribunale di Agrigento, in sede di rinvio conseguente alla sentenza della Corte di cassazione che aveva cassato la decisione di primo grado di annullamento del provvedimento del Garante 9 febbraio 2012, n. 53 (doc. web n. 1901698), ha confermato quest'ultimo, in ragione del quale era stata sanzionata una banca per omessa informativa in relazione ad un impianto di videosorveglianza e ad uno di rilevazione di dati biometrici nonché per omessa notificazione del trattamento al Garante (3 marzo 2017, n. 377).

In altro caso, una società è stata sanzionata per aver effettuato un trattamento dati mediante l'invio di una *e-mail* promozionale in assenza di informativa e consenso, violazione per la quale era stata già destinataria di un precedente provvedimento prescrittivo/inibitorio e già sanzionata con un provvedimento ingiuntivo. L'organo giudicante ha confermato il provvedimento del Garante dell'8 maggio 2013, n. 237 (doc. web n. 2640483), riducendo la sanzione al minimo edittale in virtù delle modalità con le quali era avvenuto il trattamento (Trib. Siena, 20 dicembre 2016, n. 180).

In altro caso, ad un esercizio commerciale è stata confermata la sanzione imposta dal Garante con provvedimento 7 maggio 2015, n. 278 (doc. web n. 4207992) per aver omesso di rendere l'informativa mediante apposito cartello di segnalazione della presenza di videosorveglianza nel locale, nell'erroneo presupposto che i due distinti locali da cui era composto (bar e sala giochi) costituissero un'unica attività (Trib. Brescia, 1° marzo 2017, n. 614).

Notificazione

Cinque pronunce hanno affrontato il tema della notificazione prevista dall'art. 37 e ss. del Codice.

In un caso, la Corte di cassazione ha accolto il ricorso del Garante avverso la sentenza del Tribunale di Ravenna che aveva annullato un'ordinanza ingiunzione del 2 febbraio 2012, n. 43 (doc. web n. 2109706), per omessa notificazione ex art. 37 del Codice nei confronti di una casa di cura, ritenendo che le banche dati dei pazienti delle strutture sanitarie in cui confluivano, insieme agli altri dati idonei a rivelare lo stato di salute, ivi compresi quelli relativi a malattie mentali, infettive e diffusive rientrano nella nozione di insiemi organizzati di informazioni gestiti da strutture anziché da persone fisiche e dunque sono soggette a notificazione (9 gennaio 2017, n. 188).

Tre opposizioni hanno riguardato l'omessa notificazione del trattamento di dati biometrici per il rilevamento delle presenze del personale dipendente.

In un caso, su impugnazione di un istituto di istruzione secondaria, l'organo giudicante ha confermato il provvedimento del Garante 30 maggio 2013, n. 262 (doc. web n. 2503101), ritenendo che le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità (Trib. Taranto, 20 settembre 2017, n. 2384).

In un'altra pronuncia, il Tribunale di Cosenza ha annullato la sanzione relativa all'omessa richiesta di verifica preliminare, riconoscendo la buona fede del trasgressore, mentre ha ritenuto che la notifica al Garante fosse doverosa, in quanto non è necessaria la memorizzazione delle impronte digitali costituenti i dati biometrici essendo sufficiente un'attività di raccolta ed elaborazione temporanea dei dati, così confermando il provvedimento del Garante 25 giugno 2015, n. 381 (doc. web n. 4261166) ma rideterminandone la sanzione con l'applicazione dell'ipotesi attenuata della minore gravità (24 novembre 2016, n. 24888).

Quest'ultima argomentazione è stata posta alla base di un'altra pronuncia del Tribunale di Patti (9 novembre 2017, n. 700) in riferimento al sistema di rilevamento dati biometrici adottato da un ente, confermando per il resto il provvedimento del Garante 25 novembre 2015, n. 620 (doc. web n. 4893688).

Nell'ultimo caso il Tribunale di Roma, in sede di giudizio di rinvio stabilito dalla Corte di cassazione, ha confermato il provvedimento del Garante 8 novembre 2007, n. 61, stabilendo che ad un laboratorio di analisi cliniche non può applicarsi l'esimente dell'errore scusabile, non potendo i dubbi interpretativi sull'obbligo della notificazione tradursi in buona fede e in ipotesi di *ignorantia legis* (26 maggio 2017, n. 10821).

Trattamento dati da parte di soggetti pubblici

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

Due casi hanno riguardato la pubblicazione di dati sensibili su siti istituzionali.

Nel primo caso, il Tribunale di Avellino, in sede di rinvio su ricorso davanti alla Corte di cassazione proposto dal Garante a difesa del provvedimento 9 settembre 2010 (doc. web n. 1782024), ha accolto l'opposizione di un ente territoriale che aveva diffuso dati idonei a rivelare lo stato di salute tramite pubblicazione di graduatorie riguardanti disabili sul proprio sito istituzionale, ritenendo sussistere la buona fede essendo l'ignoranza dovuta ad elementi e circostanze di natura positiva: nel caso di specie la sanzione era sopravvenuta dopo la pubblicazione, inizialmente lecita in quanto effettuata in vigenza di disposizione di legge che qualificava come pubbliche le graduatorie in esame e di un provvedimento del Garante in cui si richiedeva di individuare forme idonee per garantire la trasparenza e la conoscibilità anche attraverso l'utilizzo delle tecnologie telematiche (15 maggio 2017, n. 947).

Nel secondo caso, è stato annullato il provvedimento del Garante 5 marzo 2015, n. 124 (doc. web n. 3986892) e accolto il ricorso proposto da un istituto scolastico che aveva pubblicato sul proprio sito web i dati personali di alunni con disabilità, riconoscendo superata la presunzione di colpa, in quanto la circolare pubblicata, a differenza delle altre dello stesso periodo, non indicava la destinazione al sito web dell'istituto, dovendo presumibilmente la pubblicazione imputarsi ad errore di un docente responsabile della gestione del sito (Trib. Venezia, 29 settembre 2015, n. 3155).

In altra opposizione il Tribunale di Torre Annunziata ha confermato il provvedimento Garante 4 giugno 2015, n. 338 (doc. web n. 4562454), che ha sanzionato un Comune per non aver aggiornato il documento programmatico sulla sicurezza, né aver designato gli incaricati del trattamento dei dati (22 novembre 2017, n. 2964).

È stato accolto il ricorso proposto da una casa circondariale sanzionata con il provvedimento del Garante 17 settembre 2015, n. 483 (doc. web n. 4642360) per aver imposto che il certificato medico prodotto dai dipendenti dell'amministrazione specificasse la non sussistenza di patologie afferenti lo stato psichico, ritenendo il giudice che il diritto alla riservatezza debba essere contemperato con le esigenze proprie dell'attività di istituto che, nel caso specifico, potevano essere compromesse da

eventuali disagi di natura psichiatrica dell'agente penitenziario (Trib. Pisa, 6 giugno 2017, n. 5473).

Infine, un comune è stato sanzionato dal Garante con provv. 21 gennaio 2016, n. 15 (doc. web n. 5148981), per aver comunicato, in assenza di norma di legge o di regolamento, dati personali relativi a terzi a soggetti non coinvolti nel procedimento amministrativo sanzionatorio relativo ad una violazione del limite massimo di velocità. Nella fattispecie, il comune aveva inviato al trasgressore, su sua richiesta, la documentazione fotografica del misuratore elettronico in cui compariva il volto di un terzo soggetto a bordo del veicolo transitante in senso contrario. Il giudice ha confermato integralmente il provvedimento del Garante (Trib. Rovigo, 11 ottobre 2017, n. 758).

Ulteriori casi

Due casi hanno riguardato l'inosservanza di un provvedimento del Garante.

Nel primo caso, l'organo giudicante ha confermato il provvedimento del Garante 15 febbraio 2012, n. 472 (doc. web n. 188523), che aveva sanzionato una compagnia telefonica per non aver rispettato il divieto emesso dallo stesso Garante, sia in relazione alla conservazione dei dati di traffico telefonico e telematico oltre i termini previsti, sia per aver consentito ad altra società l'accesso ai dati in assenza di una nomina della stessa quale responsabile del trattamento (Trib. Cagliari, 28 giugno 2017, n. 2147).

In altro caso il giudice adito (Trib. Cuneo, 20 giugno 2017, n. 614) ha confermato integralmente il provvedimento del Garante 8 maggio 2014, n. 231 (doc. web n. 3275922) relativo a una società che offriva servizi a pagamento su internet e sanzionata dal Garante per aver ceduto i dati acquisiti a terzi in assenza di consenso e informativa degli interessati; per tali dati era stato altresì emesso un divieto di trattamento che la società in questione non aveva osservato ed era stata riscontrata anche una violazione per non aver la stessa dato pieno riscontro alle richieste di informazioni formulate dall'Autorità; inoltre era stata applicata la sanzione prevista in relazione alle banche dati di particolare rilevanza e dimensioni.

La Corte di cassazione si è occupata del termine di 90 giorni entro i quali, in base all'art. 14 della legge n. 689/1981, deve avvenire la notifica agli interessati degli estremi della violazione. Riprendendo la giurisprudenza costante, per la quale la durata del procedimento va valutata in relazione al caso concreto e alla sua complessità, è stata confermata la sentenza del Tribunale di Milano che ha individuato il *dies a quo* per il computo dei 90 giorni nel ricevimento delle deduzioni difensive da parte dell'interessata, confermando il provvedimento del Garante 21 dicembre 2011, n. 499 (doc. web n. 1880564) (25 maggio 2017, n. 25890).

Tra le sentenze che hanno riguardato la violazione di misure minime di sicurezza, se ne segnala una che, pur riducendo la sanzione, ha confermato il provvedimento del Garante 1° ottobre 2015, n. 514 (doc. web n. 4612053), poiché l'ente locale ricorrente, con riferimento ad un impianto di videosorveglianza installato presso la propria sede, non aveva predisposto un'apposita informativa, né aveva designato gli incaricati del trattamento, non essendo stata ritenuta sufficiente al riguardo la generica disposizione regolamentare dell'ente che considera tali tutti gli operatori che effettuano raccolta di immagini per mezzo di sistemi di videosorveglianza (Trib. Trieste, 7 dicembre 2016, n. 905).

Analogamente, è stata respinta l'impugnazione avverso la sanzione comminata con provvedimento del Garante 12 novembre 2015, n. 591 (doc. web n. 4845512), ad un esercizio commerciale dotato di un impianto di videosorveglianza che, oltre a non aver nominato incaricati e responsabili del trattamento e non aver predisposto un'informativa idonea (poiché posta all'interno del locale e non visibile dall'esterno), non aveva attuato tutti gli adempimenti necessari in materia di controllo a distanza dei lavoratori (Trib. Napoli, 24 febbraio 2017, n. 4222).

In due casi, due distinte società sono state sanzionate per aver conservato le

immagini riprese da telecamere di videosorveglianza oltre il termine previsto dal provvedimento del Garante in materia.

Nel primo, il Tribunale di Trento (8 novembre 2016, n. 1067) ha stabilito che persiste la responsabilità del titolare a vigilare sul rispetto del termine anche a seguito della designazione di un responsabile e che l'assunzione della veste di titolare del trattamento impone l'onere di avvalersi delle nozioni tecniche per poter svolgere quel compito, confermando il provvedimento del Garante 8 luglio 2015, n. 414 (doc. web n. 4240779).

Nel secondo caso, il giudice, confermando il provvedimento del Garante 25 febbraio 2016, n. 80 (doc. web n. 5422795), ha stabilito che può ritenersi ammissibile l'allungamento dei tempi di conservazione delle immagini di un sistema di videosorveglianza posto all'interno di una sala giochi fino ad una settimana, in quanto si tratta di attività caratterizzata dall'alto rischio per il numero di persone che la frequentano e la quantità di denaro circolante, mentre per tempi di conservazione superiori alla settimana, come nel caso di specie, sarebbe stata necessaria una richiesta di verifica preliminare da sottoporre al Garante che invece non si è riscontrata (Trib. Milano, 15 giugno 2017, n. 6684).

Diritto alla corretta rappresentazione dell'identità personale

Due pronunce hanno riguardato la richiesta di deindicizzazione di determinate pagine web proposta dagli interessati nei confronti di due distinti primari motori di ricerca e del sito fonte delle notizie.

Nel primo caso, il giudice ha confermato il provvedimento del Garante 12 marzo 2015, n. 153 (doc. web n. 4006210), che aveva negato la sussistenza dei presupposti per l'esercizio del diritto all'oblio in presenza di un prevalente interesse pubblico a conoscere possibili irregolarità nelle assunzioni in un'azienda municipalizzata. In particolare, il giudice ha riconosciuto che l'appartenenza, pur risalente nel tempo, del ricorrente ad un movimento politico costituisse un elemento rilevante e che la nozione di "ruolo nella vita pubblica", precisata dalle linee guida come circostanza in grado di comprimere il contrapposto diritto alla *privacy*, ha un ampio significato, ricomprendendo qualunque attività o incarico che si svolga in un settore di interesse per il pubblico e comporti l'esercizio di funzioni pubbliche o anche solo l'utilizzo di risorse pubbliche (Trib. Milano, 2 marzo 2017, n. 2506).

Nel secondo caso, il giudice ha respinto l'impugnazione della decisione del Garante del 25 febbraio 2016, n. 83 (doc. web n. doc. web n. 4881581), che aveva accolto la richiesta dell'interessato, residente in Italia, di deindicizzazione di alcuni *link* a risultati di una ricerca effettuata a partire dal suo nome ritenuti lesivi e non più attuali, nei confronti di un motore di ricerca insediato in Irlanda, che contestava la competenza del Garante e del Tribunale, nonché l'applicazione della legge italiana (Trib. Milano, 5 gennaio 2016, n. 12632).

Nel terzo caso, è stato confermato il provvedimento del Garante 21 aprile 2016, n. 186 (doc. web n. 5146011), che non ha accolto la richiesta di deindicizzazione dell'interessato in quanto il fatto rappresentato, pur risalente nel tempo, aveva avuto recenti sviluppi giudiziari, ravvisando, in particolare l'essenzialità dell'informazione riguardo a fatti di interesse pubblico, in virtù del tipo di reato, perpetrato nei confronti di organi dello Stato, e della sua entità benché il ricorrente non fosse un personaggio pubblico (Trib. Milano 26 gennaio 2017, n. 982).

Varie

Una pronuncia, che ha riguardato l'esercizio del diritto di accesso ai dati personali, accogliendo l'impugnazione avverso il provvedimento del Garante 31 gennaio 2013, n. 46 (doc. web n. 2355191), ha affermato che la richiesta di accesso avanzata da un cliente di conoscere tutti gli estratti di conto corrente di un determinato arco temporale con un istituto bancario, rientra nell'ambito di applicazione del testo unico bancario e non dell'art. 7 del Codice, come invece sostenuto dal Garante (Trib. Crotone, 24 settembre 2013, n. 821).

In un altro caso, un dipendente di un ente territoriale aveva inviato al datore di lavoro una *e-mail* di un collega acquisita nell'ambito di una *mailing list* sindacale. L'interessato, che in relazione al contenuto della *e-mail* è stato sottoposto ad un procedimento disciplinare, lamentava l'indebito utilizzo della *e-mail* da parte dell'amministrazione. L'organo giudicante, confermando, quanto all'esito, il provvedimento del Garante 20 aprile 2017, n. 202 (doc. web n. 6552839), che non aveva ravvisato illiceità del trattamento, ha ritenuto che la *e-mail* non costituisse un dato personale, bensì una mera dichiarazione del ricorrente, per cui la pretesa di blocco dei dati nei confronti dell'ente è stata ritenuta infondata (Trib. Torino, 8 novembre 2017, n. 5351).

In altro caso, una società ha proposto ricorso avverso il provvedimento d'urgenza del Garante 6 ottobre 2016, n. 389 (doc. web n. 5508051) con cui era stata disposta nei confronti della stessa la misura temporanea del blocco del trattamento dei dati contenuti in una biobanca comprendente campioni biologici e dati personali e sensibili relativi a circa 11.700 individui abitanti in una specifica zona. La società aveva acquistato la suddetta banca dati da altra società in fallimento omettendo di richiedere il consenso agli interessati per il successivo trattamento dati connesso all'attività di ricerca. Il Tribunale di Cagliari ha accolto il ricorso, ritenendo valido il consenso a suo tempo espresso dagli interessati nei confronti della società fallita, perseguendo la ricorrente le medesime finalità di ricerca scientifica e potendo gli interessati esercitare i propri diritti in conformità alle disposizione del Codice. Il Tribunale ha altresì ordinato al Garante la pubblicazione del dispositivo della sentenza su due quotidiani nonché sul suo sito internet (6 giugno 2017, n. 1569). Sulla pronuncia pende ricorso davanti alla Corte di cassazione.

In tema di dati biometrici, il Tribunale di Roma ha confermato il provvedimento del Garante 25 febbraio 2016, n. 77 (doc. web n. 4807744) che aveva ritenuto non conforme al Codice il sistema di riconoscimento facciale, di cui all'istanza di verifica preliminare, delle fotografie poste sui documenti d'identità dei soggetti che volessero presentare a banche o intermediari finanziari richieste di finanziamento, in quanto il trattamento suddetto non rispettava i principi di necessità e proporzionalità (3 ottobre 2017, n. 18849).

È stato confermato anche il provvedimento del Garante 22 giugno 2016, n. 275 (doc. web n. 5255159), con il quale l'Autorità ha vietato ad una società di telecomunicazioni l'ulteriore utilizzo, per finalità di *marketing*, di molteplici dati personali di terzi, in quanto illegittimamente acquisiti. L'organo giudicante ha ritenuto che l'operazione di contattare clienti che avevano negato il loro consenso ad essere contatti per attività promozionali allo scopo di acquisirne il consenso per il futuro non fosse lecito alla luce dei principi generali del trattamento dei dati (Trib. Milano, 5 maggio 2017, n. 5022).

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

Conformemente agli indirizzi giurisprudenziali e al parere espresso dall'Avvocatura generale dello Stato, il Garante, nei giudizi diversi da quelli direttamente attinenti a pronunce dell'Autorità, ha limitato la propria 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 ha comunque seguito con attenzione tutti i contenziosi nei quali non ha ritenuto opportuno intervenire, chiedendo alle avvocature distrettuali dello Stato di essere comunque informata sullo svolgimento delle vicende processuali e di riceverne comunicazione in merito agli esiti.

21 L'attività ispettiva e le sanzioni

21.1. *Gli ambiti dell'attività ispettiva*

Come è noto, l'attività ispettiva è lo strumento istruttorio necessario sia per accertare *in loco* situazioni di fatto oggetto di valutazione da parte dell'Autorità in relazione a specifici casi, sia per acquisire conoscenze in relazione a fenomeni nuovi in vista di successivi interventi da parte del Garante nell'ambito delle attribuzioni allo stesso rimesse dalla legge.

Conformemente a quanto previsto dalla direttiva 95/46/CE (e non diversamente ora dal RGPD), il legislatore nazionale ha dotato il Garante di poteri di controllo e di accertamento diversi per grado di "invasività" e per efficacia.

Da una parte, infatti, è stato previsto che il Garante possa richiedere informazioni e documenti al titolare, al responsabile, agli incaricati e anche a terzi, in base ad una "domanda-risposta" e in un'ottica di collaborazione fra organi incaricati di acquisire le informazioni e soggetti ispezionati. Dall'altra, è stato stabilito che l'Autorità possa procedere ad accessi diretti agli archivi e alle banche dati del titolare del trattamento indipendentemente dalla volontà dello stesso, e possa acquisire le informazioni e i documenti ritenuti necessari avvalendosi, se del caso, anche di strumenti di polizia giudiziaria.

Le ispezioni (275 nel 2017) sono programmate secondo linee di indirizzo stabilite dal Garante con proprie delibere che individuano gli ambiti del controllo e gli obiettivi numerici da conseguire e sono rese pubbliche attraverso il sito web del Garante, dandone anche conoscenza mediante la *newsletter* (cfr. 28 febbraio 2017, n. 425, doc. web n. 6024066 e 12 ottobre 2017, n. 433, doc. web n. 6956434); sulla base dei criteri così fissati, l'Ufficio individua i soggetti da sottoporre a controllo e istruisce i conseguenti procedimenti.

Il programma relativo al 2017 ha previsto che l'attività ispettiva fosse, tra l'altro, indirizzata ai seguenti settori:

– trattamenti di dati personali effettuati per il rilascio dell'identità federata (Spid);

– trattamenti di dati personali effettuati dall'Istat, per una verifica preliminare sul SIM (Sistema integrato di microdati) e altri sistemi informativi statistici come da parere sul programma statistico nazionale del 20 ottobre 2015;

– trattamenti effettuati da un consolato italiano all'estero tra quelli che rilasciano il maggior numero di visti e si avvalgono di soggetti esterni per la conduzione di tale attività; il controllo è stato effettuato in collaborazione con il Ministero degli affari esteri e della cooperazione internazionale;

– trattamenti di dati personali per attività di *telemarketing* effettuati sia sul territorio nazionale che in Albania; in quest'ultimo caso le verifiche sono state eseguite, con la partecipazione di personale dell'Ufficio, dall'Autorità albanese nell'ambito dell'Accordo di cooperazione con la stessa sottoscritto in data 20 febbraio 2015;

– trattamenti di dati effettuati nell'ambito dell'attività di recupero crediti.

Come specificato al successivo par. 21.3, nel periodo di riferimento le verifiche si sono soffermate anche sui seguenti ambiti:

– adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;

– adempimento dell'obbligo di notificazione da parte di soggetti, pubblici e privati, individuati mediante raffronto con il registro generale dei trattamenti;

– 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.

21.2. *La collaborazione con la Guardia di finanza*

L'Autorità ha continuato ad avvalersi della preziosa collaborazione della Guardia di finanza per lo svolgimento dell'attività di controllo. Il consolidato rapporto con il Corpo consente al Garante di disporre di risorse qualificate in grado di supportare l'attività ispettiva sull'intero territorio nazionale attraverso:

– la partecipazione di personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento;

– l'assistenza nei rapporti con l'autorità giudiziaria;

– lo sviluppo di attività ispettive delegate o subdelegate per l'accertamento delle violazioni;

– la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate;

– l'esecuzione di indagini conoscitive sullo stato di attuazione della legge in determinati settori;

– la segnalazione all'Autorità di situazioni rilevanti, ai fini dell'applicazione della legge, acquisite anche nell'esecuzione di altri compiti di istituto.

A tal fine il Nucleo speciale *privacy*, istituito nel settore del Comando unità speciali della Guardia di finanza, provvede direttamente, sulla base di un apposito protocollo d'intesa (rinnovato nel 2016), ad effettuare gli accertamenti sull'intero territorio nazionale, avvalendosi anche del Nucleo speciale frodi tecnologiche e, ove necessario, degli altri reparti del Corpo territorialmente competenti. A mente del RGPD, nel protocollo è stato altresì previsto che il Garante possa avvalersi di personale specializzato di tale Corpo per la conduzione di ispezioni congiunte con altre Autorità estere.

Le informazioni e i documenti acquisiti nell'ambito degli accertamenti vengono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge. Qualora nell'ambito dell'ispezione emergano violazioni penali o amministrative, la Guardia di finanza procede direttamente alla segnalazione della notizia di reato all'autorità giudiziaria – nel periodo di riferimento ciò è avvento per n. 16 violazioni penali – o alla contestazione della sanzione amministrativa in conformità alla legge 24 novembre 1981, n. 689, circostanza che ha avuto luogo per n. 359 violazioni amministrative.

Da un punto di vista più strettamente operativo, l'adozione del protocollo ha consentito: 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 della 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 speciale frodi tecnologiche della Guardia di finanza in attività ispettive o di analisi ad alto contenuto tecnico/informatico.

La consolidata cooperazione si estrinseca anche in attività formative rivolte al

personale del Corpo al fine di approfondire la conoscenza delle disposizioni del Codice e dei provvedimenti dell'Autorità: entro questa cornice va collocato l'incontro congiunto con il Nucleo speciale *privacy*, con una delegazione dell'Autorità di protezione dei dati, del Ministero dell'interno e della Direzione di polizia della Repubblica del Montenegro, sul tema "*inspection methodology*", nell'ambito dell'iniziativa di assistenza denominata "*Project IPA 2013 Western Balkans: Fight Against Organized Crime – International Cooperation in Criminal Justice"* (24 maggio 2017).

21.3. *I principali settori oggetto di controllo*

Oltre a quanto già riportato al paragrafo 21.1, le ispezioni effettuate dall'Autorità nel 2017 hanno riguardato le seguenti categorie di titolari del trattamento:

– società operanti nel settore dell'intermediazione creditizia, della concessione di prestiti e dei servizi finanziari, anche con riferimento alla concessione di prestiti finalizzati (ed ai dati eventualmente raccolti anche attraverso l'utilizzo di siti internet). Particolare attenzione è stata dedicata ai trattamenti di dati effettuati nell'ambito dei sistemi di informazioni creditizie funzionali a definire il profilo o la personalità della clientela o ad effettuare controlli sulla referenza creditizia (es., accesso banche dati Sic o Scipafi);

– società che offrono servizi di vendita a domicilio, con specifico riguardo ai dati personali raccolti attraverso l'utilizzo di siti internet e, in particolare, alle modalità di informativa all'interessato e di acquisizione del consenso, che deve rivestire il carattere della specificità in relazione alle diverse finalità perseguite (ivi comprese quelle promozionali, anche con modalità automatizzate ai sensi dell'art. 130 del Codice);

– società operanti nel settore della cd. *sharing economy*, per la verifica delle modalità di informativa all'interessato e di acquisizione del consenso dello stesso, nonché dell'eventuale notificazione del trattamento e delle misure di sicurezza adottate, con specifico riguardo ai dati dei clienti raccolti nell'ambito dei servizi *online*;

– centri odontoiatrici, per la verifica delle modalità di informativa all'interessato e di raccolta del consenso dello stesso in relazione all'acquisizione di dati sensibili, nonché, nel caso di appartenenza del centro ad un gruppo societario, per l'esame dei flussi dei dati dei pazienti tra le diverse società del gruppo e la verifica del relativo rispetto degli eventuali obblighi e delle misure di sicurezza necessarie;

– società che offrono servizi di informazioni commerciali, al fine di verificare il rispetto degli obblighi relativi all'informativa e al consenso degli interessati e l'adozione delle misure di sicurezza, nonché, nel caso di società di informazioni commerciali di maggiori dimensioni, le modalità con le quali si garantisce il riscontro telematico alle richieste di accesso ai dati personali avanzate dalle persone censite e le banche dati utilizzate per il recupero crediti, nonché le misure adottate al fine di dare attuazione alle prescrizioni del Garante;

– centri di assistenza agricola locale facenti capo a diversi centri di assistenza agricola nazionali, per la verifica del trattamento dei dati personali dei propri assistiti, con particolare riferimento alle modalità di attuazione delle misure, anche organizzative, previste dall'art. 116 del Codice – Conoscibilità di dati su mandato dell'interessato – ed alle deleghe per accedere a banche dati di terzi (es., Anagrafe tributaria, Inps, Comuni), comprensive delle relative manifestazioni di specifico consenso da parte dell'interessato/assistito;

– Asl, Aziende ospedaliere ed altri enti sanitari pubblici, in relazione ai trattamenti di dati personali effettuati mediante il cd. *dossier* sanitario, con particolare

riferimento alle modalità di rilascio dell'apposita informativa agli interessati e di acquisizione dello specifico consenso, nonché alle modalità predisposte dal titolare del trattamento per l'autenticazione del personale sanitario ai fini dell'accesso al *dossier*, ai sistemi di controllo delle operazioni effettuate, alle modalità di registrazione automatica di appositi *file* di log, al periodo di conservazione dei log stessi, alle modalità di rilevazione di eventuali anomalie negli accessi e alle relative modalità di verifica e controllo, alle misure adottate al fine di garantire all'interessato l'effettivo esercizio dei diritti di cui all'art. 7 del Codice, tra cui quelli di revoca del consenso all'implementazione del *dossier*, di oscuramento di alcuni specifici eventi clinici o di visione degli accessi avvenuti al proprio *dossier* sanitario;

– società organizzatrici di concorsi a premio, in relazione all'eventuale utilizzo a fini di profilazione dei dati personali dell'interessato, all'ambito e alle modalità di comunicazione a terzi dei dati, con particolare riferimento alle comunicazioni tra l'Amministrazione autonoma dei monopoli di Stato, altri soggetti pubblici e Sogei s.p.a.;

– società che offrono servizi di ricerca e selezione del personale, anche mediante l'utilizzo di siti web, per finalità di mediazione tra domanda ed offerta di lavoro (ai sensi del decreto legislativo 10 settembre 2003, n. 276 "Attuazione delle deleghe in materia di occupazione e mercato del lavoro", della legge 15 luglio 2011, n. 111 "Disposizioni urgenti per la stabilizzazione finanziaria", nonché della legge n. 68/1999 "Norme per il diritto al lavoro dei disabili"), in relazione ai trattamenti di dati personali effettuati per l'erogazione del servizio e con particolare evidenza per il trattamento di dati sensibili; società operanti in vari settori, al fine di verificare le modalità del trattamento dei dati personali dei propri dipendenti effettuato mediante sistemi di geolocalizzazione installati a bordo di automezzi aziendali, nonché i presupposti di legittimità per l'adozione di tali sistemi, con particolare riferimento alle modalità di attuazione delle disposizioni di cui all'art. 4, l. n. 300/1970;

– società operanti in vari settori, al fine di verificare le modalità di trattamento dei dati personali raccolti attraverso l'utilizzo di siti web, l'eventuale raccolta di dati sensibili degli interessati, nonché le modalità di adempimento degli obblighi di rilascio dell'informativa e di raccolta del consenso degli interessati, specifico per le distinte finalità per cui i dati sono raccolti (ad es., *marketing*, comunicazione dei dati a soggetti terzi, profilazione).

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.

21.4. *I provvedimenti adottati a seguito dell'attività ispettiva*

Attraverso le ispezioni l'Autorità svolge un'incisiva attività istruttoria finalizzata a uno o più dei seguenti obiettivi:

– intervenire sui trattamenti illeciti da chiunque effettuati adottando i provvedimenti cautelari previsti dalla legge (blocco e divieto) e/o prescrivendo le misure necessarie per rendere il trattamento conforme alla legge (contrasto dell'illecito);

– verificare lo stato di attuazione 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 delle finalità sottese, l'ispezione è comunque 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 violazioni eventualmente rilevate.

Con riferimento al 2017, tra i provvedimenti più rilevanti adottati dal Garante sulla base degli elementi istruttori acquisiti in sede ispettiva, si segnalano, in ordine cronologico, i provvedimenti con i quali il Garante ha:

– prescritto ad uno dei maggiori operatori telefonici nazionali – all'esito della definizione di un procedimento conseguente ad un reclamo relativo all'ingiustificata attivazione, all'insaputa dell'interessato, di un numero elevato di linee di telefonia residenziale (oltre 800) – alcune misure necessarie al fine di individuare, in tutti i sistemi della società, eventuali erronee discordanze tra i dati riferiti a intestatari di linee telefoniche e intestatario delle relative fatture e, conseguentemente, ad adottare i necessari rimedi (provv. 6 aprile 2017, n. 176, doc. web n. 6376175);

– prescritto ad un altro dei maggiori operatori telefonici nazionali di informare senza ritardo tutti gli interessati che non fossero già stati informati, della violazione dei dati personali che li ha riguardati e che ha coinvolto alcune migliaia di clienti della società (provv.ti 11 maggio 2017, n. 226, doc. web n. 6431926 e 26 luglio 2017, n. 343 doc. web n. 6821202);

– vietato, ad una società di consulenza, formazione e assistenza tecnica, l'ulteriore trattamento per finalità di *marketing* dei dati personali degli interessati acquisiti illecitamente (provv. 30 novembre 2017, n. 503, doc. web n. 7522090);

– prescritto ai titolari del trattamento dei siti web riferibili ad un partito politico le misure necessarie per la sicurezza informatica, nonché alcune integrazioni in merito all'informativa resa agli interessati ed alle modalità di acquisizione del consenso degli stessi, avendo l'Autorità rilevato la parziale inidoneità dell'informativa utilizzata e l'illiceità del trattamento dei dati personali degli utenti in ragione della comunicazione a soggetti terzi dei dati medesimi in mancanza di idoneo presupposto (provv. 21 dicembre 2017, n. 548, doc. web n. 7400401).

Relativamente ad alcuni 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.

21.5. *L'attività sanzionatoria*

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

Nel 2017, in relazione alle istruttorie effettuate, sono state inviate 41 segnalazioni di violazioni penali all'autorità giudiziaria, di cui:

– dodici per la mancata adozione delle misure minime di sicurezza;

– otto per trattamento illecito dei dati;

– sei per inosservanza di un provvedimento del Garante;

– cinque per violazioni della l. n. 300/1970, punite come reato dall'art. 171 del Codice;

– dieci 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 ormai "metabolizzati" sia dalle imprese che dagli enti pubblici. 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.

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 appare opportuno richiamare una rilevante sentenza della Corte di cassazione penale (n. 1986/2015) che ha affrontato, respingendola, la questione di legittimità costituzionale dell'art. 169 del Codice, in riferimento agli artt. 2, 3, 21, 24, 25 della Costituzione. Nella motivazione si legge infatti che "non sussiste […] alcun contrasto di tale disposizione con gli artt. 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 "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.

Anche nel 2017 si è avuta un'incidenza non trascurabile dell'accertamento di violazioni penali relative allo Statuto dei lavoratori. 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) ed al divieto di indagini sulle opinioni ai fini dell'assunzione (art. 8), costituisce 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 decreto legislativo 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 (art. 171 del Codice).

In questo ambito, limitando la riflessione alle modifiche apportate alla parte sanzionatoria, ovvero alla formulazione dell'art. 171 del Codice: "La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'art. 38 della legge 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 man-

canza 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 lavoratore 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 venuta 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.

Nell'ambito giuslavoristico della corretta applicazione delle norme contenute nello Statuto dei lavoratori, richiamate e sanzionate dal Codice, il Garante è intervenuto in più occasioni nel 2017; in particolare, ha dichiarato illecito il trattamento di dati personali dei dipendenti di una società realizzato mediante un sistema utilizzato per la gestione delle attese della clientela allo sportello (provv. 16 novembre 2017, n. 479, doc. web n. 7355533) ed ha autorizzato, all'esito di un'istanza di verifica preliminare, il trattamento di dati personali dei dipendenti attraverso la localizzazione di veicoli aziendali da parte di una società, prescrivendo alla stessa le misure necessarie da adottare ai fini della liceità di tale trattamento (provv. 16 marzo 2017, n. 138, doc. web n. 6275314).

21.5.2. Le sanzioni amministrative

Nel 2017 sono stati avviati n. 589 nuovi procedimenti sanzionatori amministrativi. All'accertamento delle violazioni amministrative previste dal Codice può procedere:

– il personale dell'Ufficio del Garante 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 novembre 1981, n. 689.

L'art. 13, l. n. 689/1981 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 accerta-

menti effettuati autonomamente da Corpi dello Stato quali la Guardia di finanza, i Carabinieri, la Polizia di Stato 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.

La garanzia di uniformità di giudizio e di interpretazione è assicurata dal fatto che la legge affida al solo Garante il compito di irrogare le 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 2017 hanno riguardato:

– n. 286 casi di trattamento illecito per violazione delle disposizioni contenute nell'art. 167 (ad es., trattamento di dati senza il consenso degli interessati; diffusione di dati sui siti internet delle p.a.; comunicazioni elettroniche indesiderate), sanzionati dall'art. 162, comma 2-*bis*;

– n. 186 casi di omessa o inidonea informativa all'interessato, sanzionati dall'art. 161;

– n. 44 casi di omessa informazione o esibizione di documenti al Garante, sanzionati dall'art. 164;

– n. 33 casi di omessa o incompleta notificazione ai sensi degli artt. 37 e 38, sanzionati dall'art. 163;

– n. 19 casi di omessa adozione delle misure minime di sicurezza di cui all'art. 33 (ad es., mancata designazione degli incaricati; violazione delle disposizioni di cui all'All. B. al Codice), sanzionati dall'art. 162, comma 2-*bis*;

– n. 6 casi di violazione del diritto di opposizione nelle forme previste dall'art. 130, comma 3-*bis* (Registro pubblico delle opposizioni), sanzionati dall'art. 162, comma 2-*quater*;

– n. 5 casi di violazione delle modalità di comunicazione all'interessato di dati idonei a rivelare lo stato di salute (previste dall'art. 84, comma 1), sanzionati dall'art. 162, comma 2;

– n. 4 casi di inosservanza di un provvedimento del Garante, sanzionati dall'art. 162, comma 2-*ter*;

– n. 4 casi di violazione di disposizioni del Codice in relazione a banche dati di particolare rilevanza o dimensioni, sanzionati dall'art. 164-*bis*, comma 2;

– n. 1 caso di mancata comunicazione al Garante, da parte di un fornitore di servizi di comunicazione elettronica accessibili al pubblico, di violazioni dei dati personali del contraente o di altra persona (cd. *data breach*), sanzionato dall'art. 162-*ter*, comma 1;

– n. 1 caso di mancata comunicazione agli interessati, da parte di un fornitore di servizi di comunicazione elettronica accessibili al pubblico, di violazioni occorse ai dati personali degli stessi (cd. *data breach*), sanzionato dall'art. 162-*ter*, comma 2.

Un approfondimento merita il sensibile scostamento del dato relativo alle n. 589 sanzioni amministrative contestate nel 2017 rispetto al dato riferito all'anno precedente (n. 2.339 violazioni riscontrate). Nel 2016, infatti, un numero rilevante di

sanzioni amministrative (pari a n. 1.818) furono irrogate in relazione alla mancata comunicazione di violazioni di dati personali (cd. *data breach*) al Garante e agli interessati. Tali sanzioni erano riconducibili ad un rilevante *data breach* occorso ad un importante operatore nazionale, fornitore di servizi di comunicazione elettronica accessibili al pubblico, il quale non aveva provveduto a comunicare tale evento né al Garante (ai sensi dell'art. 32-*bis*, comma 1, del Codice), né ai n. 1.817 interessati direttamente coinvolti dalla violazione dei propri dati personali (ai sensi dell'art. 32-*bis*, comma 2, del Codice). I suddetti comportamenti omissivi erano stati, pertanto, sanzionati dal Garante in applicazione, rispettivamente, dei commi 1 e 2 dell'art. 162-*ter* del Codice.

I procedimenti sanzionatori definiti nel 2017 con provvedimenti di ordinanza adottati dall'Autorità, relativamente a violazioni contestate (anche) negli anni precedenti al 2017 e non definite all'epoca attraverso il pagamento spontaneo in misura ridotta da parte del contravventore, sono stati n. 1.447. Di questi, n. 1.261 hanno comportato l'applicazione di una sanzione (per un ammontare complessivo di somme ingiunte pari a 13.300.600 euro) e n. 186 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.

In relazione al numero di procedimenti sanzionatori definiti nel 2017 e, in particolare, all'ammontare complessivo delle sanzioni applicate con provvedimento di ordinanza-ingiunzione (pari, come detto, a 13.300.600 euro a fronte delle sanzioni per complessivi 993.200 euro applicate nel 2016), va osservato che tali dati sono stati influenzati in maniera rilevante dalla definizione dei procedimenti sanzionatori relativi all'attività di cd. *money transfer*. In tale ambito, infatti, sono stati adottati n. 5 provvedimenti collegiali di ordinanza-ingiunzione, nei confronti di altrettante società titolari del trattamento che hanno consentito la definizione, complessivamente, di n. 1.081 procedimenti sanzionatori, con conseguente applicazione di sanzioni per 11.010.000 euro, a fronte dell'uso illecito dei dati personali riferiti ad oltre mille persone inconsapevoli (provv.ti 2 febbraio 2017, nn. 39, 40, 41, 47, 48, doc. web nn. 6009674, 6010258, 6009746, 6009876, 6010438).

Le gravi violazioni sono emerse nel corso di un'indagine della Procura della Repubblica di Roma. Il Nucleo di polizia valutaria della Guardia di finanza su delega della magistratura ha infatti accertato che una multinazionale, in concorso con altre quattro società, raccoglieva e trasferiva in Cina somme di denaro riconducibili a imprenditori cinesi, in violazione non solo della normativa antiriciclaggio, ma anche di quella sulla protezione dei dati personali, la cui violazione ha determinato l'intervento del Garante.

Per assecondare il desiderio della clientela di impedire l'associazione tra le rimesse finanziarie e i reali mittenti, le società operavano attraverso la tecnica del frazionamento (dividendo cioè le somme di denaro in più operazioni sotto la soglia prevista dalla normativa antiriciclaggio) e attribuivano i trasferimenti di denaro a più di mille clienti del tutto ignari, utilizzando illecitamente i loro dati. I nominativi ai quali erano intestati i trasferimenti non erano mai i reali ordinanti e, in alcuni casi, i moduli sono risultati compilati da persone decedute o inesistenti, oppure non sottoscritti. Gli invii di denaro, poi, venivano effettuati a pochi secondi l'uno dall'altro, per importi appena sotto soglia e indirizzati allo stesso destinatario. Inoltre, i nominativi cui erano attribuiti i trasferimenti erano tratti da fotocopie di documenti di identità, conservati in appostiti raccoglitori e da utilizzare all'occorrenza.

Alla luce dei risultati dell'indagine, il Garante, tenuto conto della gravità delle violazioni commesse dalle società, del numero delle persone coinvolte i cui dati sono stati trattati senza consenso e della rilevanza della banca dati, ha inflitto le seguenti

21

sanzioni: 5.880.000 euro alla multinazionale, 1.590.000, 1.430.000, 1.260.00 e 850.000 euro rispettivamente ad ognuna delle altre quattro società, per l'importo complessivo, sopra richiamato, di oltre 11 milioni di euro.

L'ammontare dei pagamenti effettivamente effettuati nel 2017 da parte dei soggetti nei cui confronti sono stati avviati procedimenti sanzionatori amministrativi è risultato complessivamente pari a 3.776.694 euro di cui:

– 1.385.500, pagati a titolo di definizione in via breve;

– 1.329.590, 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;

– 180.000, per la definizione, in sede amministrativa, dei procedimenti relativi alla mancata adozione delle misure minime di sicurezza;

– 881.604, quali ulteriori entrate derivanti dall'attività sanzionatoria (ad 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 attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

22 Le relazioni comunitarie e internazionali

22.1 *La cooperazione tra Autorità garanti nell'UE: il Gruppo Art. 29*

Il pacchetto di riforma UE

In vista del 25 maggio 2018, data a partire dalla quale il nuovo quadro normativo introdotto dal RGPD trova applicazione, il Gruppo Art. 29 (Gruppo) ha proseguito il lavoro già avviato nel 2016 per favorire il processo di transizione e fornire i primi strumenti atti a rendere agevole l'attuazione delle nuove regole. In linea con il programma di lavoro 2016-2018 (WP 235) e il piano d'azione del 2017, il Gruppo si è concentrato, da un lato, sull'organizzazione amministrativa interna del Comitato per la protezione dei dati e sul suo funzionamento (in particolare, curando gli aspetti relativi alle regole di procedura per le sue attività, alla struttura del suo Segretariato, alle risorse IT e al *budget*) e, dall'altro, sull'adozione di linee guida sulle novità introdotte dalla riforma e indicazioni pratiche per la sua applicazione. Il Gruppo si è riunito in plenaria cinque volte e come negli anni precedenti ha lavorato servendosi dei diversi sottogruppi di cui è composto. Sui temi di maggior impatto è stato riservato uno spazio al confronto con i diversi *stakeholder* in occasione delle consultazioni pubbliche sulle linee guida adottate – riviste e modificate alla luce dei numerosi commenti ricevuti – nonché degli incontri su temi specifici (FabLab 5 e 6 aprile e 18 ottobre 2017 sui temi del consenso, violazione dei dati, *profiling*, trasparenza e trasferimento dei dati all'estero).

Con riferimento all'approfondimento sui temi chiave del RGPD, nel 2017 sono state anzitutto adottate le versioni aggiornate di alcuni documenti già approvati nel corso del 2016 e rivisti alla luce dei commenti pervenuti a seguito delle consultazioni pubbliche.

Linee guida sul diritto alla portabilità

Così le linee guida sul diritto alla portabilità (WP 242, rev. 01, doc. web n. 6058842 e le relative FAQ, doc. web n. 6058857) illustrano le peculiarità del nuovo diritto di cui all'art. 20 del RGPD che permette agli interessati di ricevere i dati personali da loro forniti al titolare del trattamento, in un formato strutturato, di uso comune e leggibile meccanicamente, e di trasmetterli a un diverso titolare, caratterizzandolo rispetto al più tradizionale diritto di accesso ai dati personali. Obiettivo delle linee guida è di analizzare questo nuovo diritto e il suo ambito di applicazione chiarendone le condizioni di applicabilità alla luce della base giuridica del trattamento (consenso dell'interessato o adempimento di obblighi contrattuali). Il Gruppo chiarisce che il diritto alla portabilità si configura in relazione ai dati forniti consapevolmente e in modo attivo dall'interessato, nonché rispetto ai dati personali generati dalle attività svolte dall'interessato. Non può dunque essere limitato ai dati personali che sono comunicati direttamente dall'interessato (ad es., attraverso la compilazione di un modulo *online*).

Il documento sottolinea inoltre l'opportunità che sia garantita l'interoperabilità dei formati con cui i dati vengono messi a disposizione in ottemperanza a una richiesta di portabilità. È per questo che le linee guida, oltre a presentare una serie di chiarimenti sugli obblighi dei titolari e raccomandazioni su buone prassi da adottare, sollecitano i rappresentanti del settore imprenditoriale e delle associazioni di settore a collaborare per definire in modo condiviso gli *standard* e i formati interoperabili che soddisfino i requisiti del diritto alla portabilità dei dati.

22

Responsabili della protezione dei dati (Rpd)

Anche le linee guida sui responsabili della protezione dei dati (Rpd, e nella traduzione inglese *Data protection officer*, Dpo), già approvate nel dicembre del 2016, sono state adottate nella versione finale, dopo la consultazione pubblica, il 5 aprile 2017 (WP 243, rev. 01, doc. web n. 5930287 e relative FAQ).

Si tratta di un documento (concernente l'interpretazione delle ipotesi di nomina obbligatoria del Rpd, oltre che su requisiti, competenze e posizione del Rpd v. già Relazione 2016, p. 148) significativo soprattutto per i Paesi che, come il nostro, con l'entrata in vigore del RGPD, si trovano per la prima volta ad affrontare l'introduzione di una figura di primario rilievo nell'applicazione del nuovo quadro di regole, obbligatoria per i soggetti pubblici e – in ambito privato – per gli specifici trattamenti previsti dall'art. 37 del RGPD.

Dopo l'adozione delle linee guida il Garante ha pubblicato alcune FAQ, in aggiunta a quelle adottate dal Gruppo Art. 29, volte a fornire chiarimenti in particolare sui soggetti tenuti alla designazione del Rpd, sulle loro qualifiche e titoli, sulla designazione formale del Rpd e sui suoi compiti e funzioni (cfr. doc. web n. 7322110 e n. 8036793).

Linee guida sulla designazione dell'"Autorità capofila"

Il Gruppo ha altresì rivisto, sempre a seguito degli esiti della consultazione pubblica, le linee guida sulla designazione della autorità capofila (*lead authority*), che deve rivestire il ruolo di "sportello unico" nei cd. trattamenti transnazionali ove cioè, ai sensi dell'art. 4 del RGPD, il titolare o il responsabile tratti dati personali in più stabilimenti nell'UE o offra prodotti o servizi in più Paesi UE, anche a partire da un solo stabilimento.

La revisione ha portato all'adozione, il 5 aprile 2017, delle nuove linee guida (WP 244 rev.01, doc. web n. 6386159 e relative FAQ, doc. web n. 7409262) che hanno l'intento di supportare titolari e responsabili del trattamento nella corretta individuazione dell'autorità competente al fine di evitare controversie e garantire un'attuazione efficace del RGPD. Il documento si sofferma, tra l'altro, sulle questioni dell'identificazione dello stabilimento principale, del ruolo del titolare del trattamento nel giustificare la scelta dello stabilimento principale, del ruolo delle autorità di protezione dati nella verifica della corretta designazione della *lead authority* e della contitolarità del trattamento.

Linee guida in materia di *Data protection impact assessment* (Dpia)

Il Gruppo ha inoltre approfondito nuove tematiche legate all'applicazione del RGPD non affrontate nel corso del 2016.

Ha lavorato sulla cd. valutazione d'impatto – prevista dagli art. 35 e ss. – che costituisce uno degli elementi chiave della "responsabilizzazione" (*accountability* nell'accezione inglese) di titolari e responsabili, tenuti ad adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del RGPD. In base all'art. 35, infatti, i titolari sono tenuti a valutare il rischio inerente al trattamento di conseguenze negative sulle libertà e i diritti degli interessati attraverso un apposito processo di valutazione (artt. 35-36). All'esito della valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente (*supervisory authority*) per ottenere indicazioni su come gestire il rischio residuale; diversamente rispetto a quanto previsto dalla direttiva 95/46 (e dall'art. 17 del Codice) l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare le misure correttive previste dall'art. 58 (dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento).

Le linee guida in materia di valutazione d'impatto, adottate in una prima versione il 4 aprile 2017, e in quella definitiva il 4 ottobre 2017 (WP 248, rev.01, doc.

web n. 7015994) anch'esse all'esito di una consultazione pubblica, mirano ad assicurare un'interpretazione coerente delle circostanze in cui è obbligatorio realizzare una valutazione d'impatto, a chiarire tale nozione e a fornire criteri per gli elenchi delle tipologie di trattamenti soggetti al requisito della valutazione che devono essere adottati dalle Autorità di protezione dei dati ai sensi dell'art. 35, par. 4. Esse sono altresì preordinate a promuovere la redazione di elenchi comuni per l'UE delle tipologie di trattamento per le quali la Dpia è obbligatoria e di elenchi dei casi in cui essa non è necessaria; a individuare criteri comuni sulla metodologia per la realizzazione di una valutazione d'impatto e a definire quando è necessario consultare l'autorità di controllo. Forniscono, infine, raccomandazioni sulla base dell'esperienza acquisita negli Stati membri dell'UE.

Linee guida in materia di profilazione e decisioni automatizzate

Con l'adozione definitiva delle linee guida sulle decisioni automatizzate e la profilazione (WP 251, doc. web n. 8050394) avvenuta il 6 febbraio 2018 previa consultazione pubblica, il Gruppo ha chiarito le principali novità dettate dal RGPD in tale ambito.

Pur riconoscendo che la profilazione e i processi decisionali automatizzati non necessariamente hanno una connotazione negativa e possono anzi apportare benefici agli individui e alla collettività, ad esempio incrementando efficienza e risparmiando risorse, il Gruppo sottolinea che occorre tuttavia essere pienamente consapevoli dei rischi significativi sui diritti delle persone che possono derivare da tali trattamenti. La loro intrinseca opacità, la possibilità che da essi derivino stigmatizzazione, discriminazione, rappresentazioni inaccurate dell'individuo, negazione di servizi o beni, mostrano la necessità di una tutela rafforzata dei diritti degli interessati rispetto agli effetti di decisioni automatizzate e profilazione.

Il documento si sofferma sulla definizione di profilazione (art. 4, par. 4), traccia le differenze tra quest'ultima – che costituisce un trattamento di dati cui si applicano tutti i principi di protezione dati compresi i requisiti di liceità di cui all'art. 6 – e le decisioni, basate unicamente sul trattamento automatizzato, che producono effetti giuridici sulla persona o su di essa incidono in modo significativo. Per le decisioni automatizzate, l'art. 22 del RGPD ne prevede infatti il divieto, fatte salve le eccezioni previste dal secondo comma dello stesso art. 22, ove cioè la decisione sia necessaria alla conclusione o esecuzione di un contratto, ove sia autorizzata dalla legge o si basi sul consenso esplicito dell'interessato.

Il documento fornisce a tal proposito chiarimenti su cosa debba intendersi per "effetti giuridici" ed "effetti significativi sulla persona", si concentra inoltre sui diritti dell'interessato e, in particolare, sul diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Il documento si sofferma infine sulle disposizioni del RGPD in materia di minori, sottolineando che, anche nell'ambito della profilazione e delle decisioni automatizzate, i minori meritano una protezione dei dati rafforzata a fronte della loro più limitata consapevolezza riguardo ai rischi che derivano dai trattamenti che li riguardano.

Linee guida in materia di consenso

Altro tema ragguardevole, già di particolare rilevanza nella direttiva 95/46, ma ora rafforzato nella nuova normativa europea, è il consenso dell'interessato, oggetto anch'esso di linee guida approvate dal Gruppo il 28 novembre 2017 e sottoposte a consultazione pubblica in vista della loro versione definitiva adottata il 10 aprile 2018 (WP 259, rev.01, doc. web n. 8668432). Il documento – che muove dal parere del Gruppo 15/2011 (WP 187, doc. web n. 2572791) – mira a segnalare i punti di novità del consenso alla luce del RGPD e fornisce chiarimenti sui requisiti per comprovarne la manifestazione. Le linee guida sottolineano che il consenso può

costituire una valida base giuridica del trattamento solo ove sia frutto di una libera scelta dell'interessato. A tal fine il documento si incentra sui requisiti che lo rendono "liberamente prestato", "informato" e sulla sua "granularità".

Le linee guida si soffermano inoltre sulla consenso condizionato, in particolare in base all'art. 7, par. 4, RGPD, secondo cui, per assicurare che il consenso sia stato liberamente prestato, occorre verificare che l'esecuzione di un contratto (compresa la prestazione di un servizio) non sia condizionata alla manifestazione del consenso rispetto al trattamento di dati non necessario all'esecuzione di tale contratto. Le stesse chiariscono il rapporto tra il "consenso dell'interessato" – che ai sensi dell'art. 4, par. 11 – deve essere una manifestazione inequivocabile di assenso (ad esempio una dichiarazione o azione positiva) e il cd. consenso esplicito necessario in specifici casi previsti dal RGPD (art. 9 nel caso in cui il trattamento riguardi dati sensibili, art. 22 per le decisioni automatizzate, e art. 49 per i trasferimenti di dati in assenza di garanzie adeguate); si soffermano sulle modalità per dimostrare la sussistenza del consenso e per garantirne la revocabilità, nonché su alcune specifiche norme del RGPD, in particolare sulle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione (art. 8) e sul consenso nell'ambito della ricerca.

Linee guida in materia di trasparenza

Parallelamente il Gruppo ha altresì lavorato sul tema della trasparenza nel trattamento dei dati personali, oggetto di specifiche linee guida, adottate il 29 novembre 2017 e sottoposte a consultazione pubblica (WP 260, rev. 01, doc. web n. 8668477). La trasparenza, come emerge da tale documento, costituisce un obbligo fondamentale per i titolari che, ai sensi dell'art. 12, devono fornire all'interessato tutte le informazioni relative al trattamento in forma concisa, trasparente, intelligibile, facilmente accessibile e con linguaggio chiaro, specie ove il trattamento riguardi minori.

Il documento fornisce esempi pratici affinché sia garantita un'efficace informativa. Sottolinea che non sussiste una reale differenza di *status* tra le informazioni che devono essere fornite in base al par. 1 e quelle da fornire ai sensi del par. 2 degli artt. 13 e 14 del RGPD. Fornisce una guida interpretativa sui requisiti previsti dall'art. 12 e chiarisce gli aspetti pratici per adempiere all'obbligo di trasparenza, ad esempio la tempistica dell'informativa e la possibilità che siano a tal fine adoperati diversi mezzi (orale, elettronico, ecc.), incluse le rappresentazioni iconografiche previste dal RGPD. Si concentra su alcuni specifici obblighi di informativa per particolari forme di trattamento, ad esempio in caso di profilazione o *data breach*.

Il documento è corredato da un'utile scheda riepilogativa che riassume gli obblighi del titolare in materia di trasparenza.

Linee guida in materia di notifica delle violazioni di dati personali

Il tema della notifica delle violazioni di dati personali (*data breach*) – già affrontato dal Gruppo in passato in relazione alla disposizione in materia di violazioni di dati prevista per i fornitori di servizi di comunicazione elettronica nell'ambito della direttiva 2002/58/CE (parere 3/2014, WP 213, doc. web n. 3815121) – ha formato oggetto di nuove linee guida, sottoposte a consultazione pubblica, volte a fornire indicazioni specifiche in ordine all'applicazione degli obblighi di notificazione che il RGPD ora impone a tutti i titolari laddove si verifichi una violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche (WP 250, rev.01, doc. web n. 8050516).

Il documento, anche attraverso numerosi esempi, fornisce indicazioni per identificare una violazione dei dati – soffermandosi, in particolare, sulle violazioni della cd. disponibilità dei dati (*availability breach*) – e sulla tempistica per procedere alla notifica all'autorità di protezione dei dati (art. 33 RGPD) e agli interessati (art. 34 RGPD). In relazione alla tempistica e alle modalità per la presentazione della noti-

fica, le linee guida precisano tra l'altro che il titolare diviene consapevole del *data breach* una volta informato dal responsabile del trattamento (piuttosto che nel momento in cui tale responsabile ne viene a conoscenza) e che lo stesso, nel caso di trattamenti transfrontalieri, deve presentare la notifica all'autorità capofila (o, nel dubbio – e nel caso in cui la violazione ponga particolari urgenze o sia particolarmente significativa –, comunque all'autorità del Paese in cui si è verificato il *data breach*) che avvierà la procedura di cd. *one stop shop* (oss) coinvolgendo le altre autorità interessate. Le linee guida chiariscono anche che la notifica non è necessaria ove i dati andati perduti fossero correttamente criptati ed è disponibile una copia o un *backup* degli stessi, ma richiama l'attenzione sulla necessità che la documentazione relativa a tutte le violazioni di dati deve essere conservata dal titolare del trattamento e messa a disposizione dell'autorità di controllo ove richiesta (in conformità all'art. 33, par. 5, del RGPD).

Il Gruppo ha inoltre lavorato per individuare regole omogenee che le stesse Autorità possono seguire in caso di violazioni che abbiano un effetto transfrontaliero.

Linee guida in materia di sanzioni amministrative

Elemento centrale del nuovo regime introdotto dal RGPD è il potere riconosciuto a tutte le autorità di controllo europee di infliggere sanzioni amministrative pecuniarie in aggiunta o in luogo delle altre misure correttive dallo stesso previste (art. 58 del RGPD). A tal fine, il nuovo quadro normativo individua i criteri comuni che devono essere utilizzati per valutare l'imposizione di una sanzione e il suo importo in funzione delle circostanze di ogni singolo caso (art. 83 del RGPD). Il Gruppo ha lavorato, già dal 2016, alla redazione delle linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie (WP 253, doc. web n. 7839406) volte a fornire alle stesse autorità di controllo indicazioni utili per una prima interpretazione comune e coerente delle disposizioni rilevanti in materia. Le linee guida, pur tenendo a mente le differenze esistenti tra i sistemi degli Stati membri nell'imposizione di sanzioni amministrative, individuano i principi cui uniformare la propria azione correttiva – con l'imposizione di sanzioni equivalenti, effettive, proporzionate e dissuasive, commisurate al caso di specie – e forniscono orientamenti alle autorità di controllo su come interpretare le singole circostanze alla luce dei criteri di cui all'art. 83, par. 2, del RGPD.

Parere sul trattamento di dati personali in ambito lavorativo

Con l'adozione del parere 2/2017 (WP 249, doc. web n. 6880588), il Gruppo si è occupato del tema della protezione dei dati in ambito lavorativo, aggiornando i precedenti documenti (parere 8/2001, WP 48, doc. web n. 1390186) e il documento di lavoro sulla sorveglianza delle comunicazioni in ambito lavorativo (WP 55, doc. web n. 1609517) per rispondere alle molte sfide alla protezione dei dati, alla riservatezza e alla dignità dei lavoratori suscitate dall'impiego crescente di tecnologie che consentono un controllo sempre più capillare del personale (si pensi, per citarne solo alcune, al monitoraggio di dispositivi quali PC, telefono, *tablet*, o al caso del "*Bring-Your-Own-Device* (BYOD)" o le tecnologie "*Mobile Device Management* (MDM)", o, ancora, l'impiego di dispositivi indossabili o sistemi di geolocalizzazione dei veicoli utilizzati dai lavoratori).

Il documento, pur rifacendosi alla direttiva 95/46, si apre al nuovo scenario dettato dal RGPD, in particolare con riferimento agli obblighi cui sono tenuti i titolari, ed amplia, con l'ausilio di appositi esempi, i punti essenziali della tutela della protezione dei dati in ambito lavorativo. In particolare si afferma che: a) i datori di lavoro devono essere consapevoli della necessità di rispettare i principi di protezione dati indipendentemente dalle tecnologie utilizzate; b) i contenuti delle comunicazioni elettroniche generate in ambito lavorativo godono della stessa protezione di analoghe comunicazioni; c) il consenso del dipendente difficilmente può costituire una valida base giuridica del trattamento dei dati che lo riguardano, a fronte dell'eviden-

te squilibrio di potere contrattuale con il datore di lavoro; d) l'esecuzione del contratto e il legittimo interesse possono costituire il fondamento giuridico del trattamento, purché il trattamento sia strettamente necessario per la legittima finalità perseguita e rispetti i principi di proporzionalità e necessità; e) i dipendenti devono ricevere un'adeguata informativa in relazione a possibili forme di sorveglianza che li riguardano; f) qualunque trasferimento di dati personali relativi ai dipendenti deve essere accompagnato da un adeguato livello di protezione.

Cooperazione tra Autorità e Comitato per la protezione dei dati

Consapevole dell'impatto che le procedure di cooperazione e il meccanismo di coerenza previsto dal Capo VII del RGPD avranno sulle attività delle Autorità di controllo e della necessità di dotarsi di strumenti adeguati alla loro attuazione, il Gruppo ha proseguito i lavori volti ad approfondire l'analisi delle disposizioni ad esse relative. A tal fine ha messo alla prova, alla luce di casi ipotetici, le linee guida adottate nel 2016 in tema di assistenza reciproca, operazioni congiunte e sportello unico e i modelli comuni per la cooperazione individuando gli aspetti che necessitavano di ulteriori precisazioni e ha adottato, sempre ad uso interno, le linee guida sulle procedure d'urgenza ai sensi dell'art. 66 del RGPD.

Con il supporto del Garante europeo per la protezione dei dati (che, come previsto dal RGPD, mette a disposizione del Comitato il segretariato), il Gruppo ha inoltre proseguito le proprie attività per la predisposizione della struttura informatica necessaria ad assicurare una agevole cooperazione tra le autorità di supervisione e tra le stesse e il Comitato europeo per la protezione dei dati.

In relazione alle future competenze del Comitato, con una dichiarazione del 4 aprile 2017 sulla proposta di revisione del regolamento 45/2001 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi dell'Unione, il Gruppo ha chiesto di prevedere espressamente che il Comitato venga consultato prima della presentazione di atti normativi europei che abbiano un impatto sulla protezione dei dati e di valutare con attenzione il futuro modello di *governance* unica per la supervisione, congiunta e coordinata fra Garante europeo per la protezione dei dati (Gepd) e autorità nazionali, sui diversi sistemi e organismi europei che operano nel settore polizia e giustizia (quali, SIS II, VIS, Europol, etc.).

Dati personali e nuove tecnologie

Sono stati altresì approfonditi gli aspetti relativi alla protezione dei dati connessi alla piattaforma del Sistema di trasporto intelligente cooperativo (C-ITS) – iniziativa della Commissione europea, volta a permettere agli utenti stradali e ai gestori del traffico la condivisione di informazioni al fine di coordinare le loro azioni. Il parere (WP 252, doc. web n. 7035839), dopo aver descritto il sistema, analizza il documento di lavoro "Trattamento dei dati personali nel contesto del C-ITS" redatto da un gruppo di lavoro sulla protezione dei dati e sulla *privacy* istituito nell'ambito della medesima piattaforma e chiarisce che i dati scambiati nell'ambito del Sistema sono dati personali, enucleando i rischi che da tale trattamento possono derivare. Anche alla luce di tali rischi, il Gruppo richiama l'attenzione della Commissione sulla necessità di individuare un'idonea base giuridica e appropriate misure di sicurezza, specificando una serie di azioni che la stessa dovrà porre in essere per l'attuazione del Sistema.

Tenendo a mente le indicazioni già fornite con il proprio parere sull'utilizzo dei droni (parere 01/2015, WP 231, doc. web n. 4810724; v. Relazione 2014, p. 175), il Gruppo è tornato sull'argomento dopo la presentazione, da parte dell'Agenzia europea della sicurezza aerea (Easa), della bozza di regolamento per l'uso dei droni – aperta alla consultazione pubblica in vista della presentazione della sua versione definitiva nel 2018. In particolare, il documento adottato mette in discussione lo scopo della registrazione degli operatori dei droni e chiede una riflessione sui desti-

natari dei dati personali raccolti durante tale processo. Dubbi sono stati espressi in ordine al sistema di identificazione elettronica previsto dalla bozza di regolamento con riferimento alle modalità di funzionamento, alle sue finalità, ai soggetti cui i dati verranno trasmessi, alla conservazione dei dati raccolti.

Sempre in tema di nuove tecnologie, a seguito di una richiesta di parere pervenuta nel 2016, il Gruppo ha fornito alcune indicazioni in ordine alla bozza di codice di condotta per le applicazioni mobili nel settore della salute, promosso dalla Commissione europea. Nella lettera inviata ai promotori di tale codice il 10 aprile 2017, il Gruppo ha sottolineato la necessità di meglio definire il sistema di *governance* del codice e di controllo sulla sua effettiva applicazione da parte degli sviluppatori delle *app*; i criteri utilizzati per qualificare o meno i dati personali oggetto di trattamento come dati sulla salute; i differenti ruoli nel trattamento dei dati che possono essere svolti dallo sviluppatore; l'informativa agli interessati, il rispetto dei principi di qualità dei dati e *accountability* (che non erano stati presi in considerazione nella bozza del codice presentata al Gruppo); i presupposti per il trattamento dei dati per finalità di *marketing* e adeguate garanzie a tutela dei minori. La versione integrata e modificata del menzionato codice dovrà essere presentata nuovamente al Gruppo o, laddove i tempi non lo consentano, potrà essere sottoposta alla procedura di approvazione prevista dall'art. 40 del RGPD.

Il Gruppo ha inoltre affrontato il tema del trattamento dei dati effettuato per il tramite del *Whois*, il servizio che consente di recuperare le informazioni di registrazione per ciascun dominio. Richiamando due note già inviate nel 2006 e nel 2014, è stata ribadita a Icann – l'ente *no profit* che gestisce il sistema dei nomi a dominio di primo livello – la necessità di trovare un'adeguata base giuridica per il trattamento dei dati personali contenuti nel registro (considerando non libero il consenso richiesto ai *registrant*) e di garantire un accesso per livelli (*layered approach*) ai dati detenuti, evitando la diffusione massiva degli stessi.

Nell'ambito del Gruppo, le autorità di protezione dei dati di volta in volta interessate hanno inoltre portato avanti la cooperazione con riferimento a titolari del trattamento che operano in diversi Paesi (quali Google, Facebook, Whatsapp, Sync.me ed Uber) al fine di acquisire chiarimenti in ordine ad alcuni trattamenti effettuati e coordinarsi nelle azioni da intraprendere.

Revisione della direttiva *e-Privacy* (2002/58/EC)

A seguito della presentazione della proposta concernente un regolamento sulla vita privata e le comunicazioni elettroniche volta a rivedere la direttiva 2002/58, avvenuta il 10 gennaio 2017 da parte della Commissione, il Gruppo ha adottato il parere 1/2017 (WP 247, doc. web n. 6880558) con il quale, nell'apprezzare sia la scelta del regolamento come strumento normativo sia l'estensione dell'ambito di applicazione del proposto regolamento ai fornitori di servizi *over the top* (OTT), ha individuato quattro aspetti di maggior rilievo: il tema del monitoraggio dell'ubicazione delle apparecchiature terminali (cd. *wi-fi tracking*), rispetto al quale si sottolinea la necessità di utilizzare in via generale e in linea con il RGPD, il consenso degli utenti, salvo casi specifici (quali la raccolta di informazioni di tipo statistico quando i dati possono essere immediatamente anonimizzati, lasciando comunque agli utenti la possibilità di opporsi); l'identificazione attenta e limitata delle condizioni per le quali l'analisi di contenuti e metadati è consentita (ovvero per finalità di sicurezza, di fatturazione o per la contestazione di fatture, per la fornitura di specifici servizi, quali assistenti virtuali per le traduzioni, etc.); la necessità che per *software* e terminali siano previste impostazioni predefinite tali da favorire il rispetto della riservatezza e chiare opzioni per confermare o modificare tali impostazioni; il divieto di creare dei muri alla navigazione (cd. *tracking walls*) se gli utenti non accettano di essere tracciati su altri siti o per la fornitura di servizi.

22

Protezione dei dati in ambito finanziario

Il parere si sofferma poi su altri aspetti che destano preoccupazione (definizione di metadati, trattamenti effettuati per finalità di *marketing* diretto, possibile adozione a livello nazionale di misure di conservazione dei dati di traffico non *targeted*) e fornisce indicazioni per contribuire ad una maggiore chiarezza del regolamento in ordine al suo ambito di applicazione.

Il Garante ha continuato a coordinare il sottogruppo "*Financial Matters*" incaricato di approfondire le diverse questioni legate all'applicazione della disciplina sulla protezione dei dati nel settore finanziario. In quest'ambito è proseguito il lavoro di approfondimento sulla ratifica nei vari Stati membri dell'Accordo Fatca (che prende il nome dalla legislazione USA antievasione fiscale *off shore*, *Foreign Account Tax Compliance Act*), in particolare completando l'attività di verifica della qualità delle misure di sua implementazione e della proporzionalità dello scambio di informazioni tra UE ed USA.

Il Gruppo ha inoltre lavorato alla preparazione di un riscontro alla petizione – presentata al Parlamento europeo, ma portata all'attenzione anche della Presidente del Gruppo – in merito alle implicazioni di Fatca sulla tutela della vita privata e sul principio di non discriminazione previsti dagli artt. 8 e 14 della Convenzione europea dei diritti dell'uomo, in particolare con riferimento all'obbligo di trasmissione dalle autorità fiscali europee a quelle statunitensi dei dati relativi ai cd. *accidental americans* e a coloro che hanno la doppia cittadinanza UE/USA (che di fatto non hanno legami effettivi con gli USA ma hanno cittadinanza sulla base dello *ius soli*).

Sempre in ambito finanziario, il Gruppo ha discusso dello stato di implementazione a livello nazionale della direttiva (UE) 2015/2366 sui servizi di pagamento (cd. PSD2) anche allo scopo di verificarne la compatibilità con il RGPD, in particolare con riferimento all'art. 94 della PSD2, che prevede che i prestatori di servizi di pagamento abbiano accesso, trattino e conservino i dati personali necessari alla prestazione dei rispettivi servizi di pagamento, solo in presenza del "consenso esplicito" dell'utente dei servizi di pagamento (laddove il RGPD fissa diverse specifiche ipotesi di trattamento in cui è necessario il consenso esplicito dell'interessato).

Il Gruppo ha inoltre continuato ad occuparsi del tema dello scambio di informazioni tra autorità di controllo dei mercati finanziari nell'ambito della loro attività di cooperazione, in particolare dialogando, in specifici incontri, con IOSCO e ESMA, le organizzazioni che, rispettivamente a livello internazionale ed europeo, riuniscono le autorità di controllo dei mercati finanziari, per discutere dei meccanismi da porre in essere affinché i trasferimenti di dati siano effettuati nel rispetto dei principi di protezione dati, specie alla luce del nuovo quadro normativo europeo. Il lavoro ha portato all'invio, il 14 giugno 2017, della lettera a ESMA (doc. web n. 8668546) sulle salvaguardie che, ai sensi dell'art. 46 del RGPD, devono essere adottate nel caso di trasferimento di dati personali dalle autorità finanziarie europee verso le omologhe di Paesi terzi – il cui ordinamento non sia stato riconosciuto come adeguato dalla Commissione europea.

La lettera sottolinea che tra i requisiti per assicurare garanzie appropriate per tali trasferimenti, il RGPD (art. 46, par. 3, lett. *b*) indica le disposizioni da inserire in accordi amministrativi tra autorità pubbliche (ad. es., un *memorandum of understanding*) che comprendano diritti effettivi e azionabili per gli interessati, previa autorizzazione dell'autorità di controllo competente.

Tali accordi tra amministrazioni devono contenere i principi base della protezione dati ed in particolare: la tutela effettiva dei diritti degli interessati, anche in via giudiziaria e con eventuale diritto ad ottenere risarcimento; il principio di trasparenza; la definizione dei concetti basilari della protezione dei dati; il principio di finalità e il divieto di utilizzi incompatibili; la proporzionalità e la necessità del trattamento,

nonché la qualità dei dati; tempi congrui di conservazione dei dati; divieto di ulteriore trasferimento, fatte salve specifiche garanzie (autorizzazione della parte che trasferisce i dati e obbligo per il terzo destinatario di assicurare le medesime salvaguardie); la sicurezza e la confidenzialità dei dati; la designazione di un meccanismo di supervisione esterna sul rispetto dei principi di protezione dati; specifiche garanzie per i dati sensibili.

Il Gruppo ha altresì avviato una prima riflessione sul tema FinTech, sottoposto ad una consultazione pubblica della Commissione europea nel mese di marzo e conclusasi a giugno 2017, dalla quale è emerso che la protezione dei dati costituisce una delle principali preoccupazioni degli *stakeholder* coinvolti. Ha infine ultimato uno studio sulla profilazione in ambito finanziario, con il quale sono state raccolte informazioni su casi nazionali ed esperienze delle varie autorità di protezione dati, anche al fine di contribuire alle linee guida sulla profilazione adottate dal Gruppo Art. 29 (WP 251, doc. web n. 8050394).

Protezione dei dati e *law enforcement*

In vista del recepimento della direttiva 2016/680 – avvenuto nell'ordinamento nazionale con il decreto legislativo 18 maggio 2018, n. 51 –, il Gruppo ha adottato un parere con il quale ha inteso fornire indicazioni su alcuni elementi essenziali della stessa (WP 258, doc. web n. 7315647).

Il documento si sofferma, in particolare, sul tema della conservazione dei dati (art. 5), richiamando l'attenzione dei legislatori nazionali sulla necessità di individuare tempi massimi di conservazione (che devono anche tenere conto delle differenti categorie di soggetti interessati) e di fissare revisioni periodiche dei dati conservati alla luce delle quali, solo per giustificati (e documentati) motivi, può esserne disposta una ulteriore conservazione. Idonee misure di *privacy by design* e *by default* dovrebbero inoltre essere adottate per consentire la cancellazione automatica dei dati una volta decorsi i termini di conservazione.

In relazione al trattamento dei dati sensibili, grande attenzione deve essere prestata al rispetto del principio di necessità e all'adozione di misure appropriate per evitare rischi di discriminazione.

Sono ribaditi il divieto generale di "decisione individuale esclusivamente automatizzata", compresa la profilazione, che abbia "effetti giuridici avversi" o "che incida significativamente" sull'interessato e la necessità che, in caso di eccezioni previste per legge, siano approntate adeguate garanzie per i diritti e le libertà delle persone interessate e sia previsto l'obbligo per i titolari di eseguire una Dpia fornendo informazioni adeguate all'interessato (salve le eventuali misure restrittive di tale diritto ai sensi dell'art. 13, par. 3, della medesima direttiva).

Raccomandazioni sono inoltre formulate in tema di diritti degli interessati (art. 13-17), conservazione dei *file* di *log* per gli accessi ai dati trattati per le finalità di *law enforcement* (art. 25) e poteri dell'autorità di supervisione (art. 47) che il Gruppo auspica coincidere con quella di supervisione competente per l'applicazione del RGPD.

Sempre in tema di *law enforcement*, alla luce della possibile presentazione di una proposta legislativa europea in materia di raccolta transfrontaliera delle prove elettroniche, il Gruppo ha adottato, il 29 novembre 2017, una dichiarazione (doc. web n. 8668240) per sollecitare, anche in tale ambito, il rispetto della disciplina in materia di protezione dei dati personali – e, in particolare, della direttiva 680/2016 – e di tenere conto dei lavori che sul tema sono in corso in seno al Consiglio d'Europa per la preparazione del Protocollo alla Convenzione di Budapest sul *cybercrime*. Il documento si sofferma anche sul tema delle richieste di accesso per finalità di *law enforcement* ai dati detenuti dai fornitori di servizi, distinguendo il caso in cui gli stessi siano stabiliti in UE da quello in cui siano fuori dall'UE. Rispetto a quest'ultima situazione si richiama l'attenzione del legislatore europeo circa la necessità di

22

evitare richieste dirette a tali soggetti al fine di scongiurare potenziali conflitti di giurisdizione e, del pari, si fa cenno alla necessità che le autorità di un Paese terzo che intendano accedere a dati detenuti da titolari del trattamento stabiliti in EU utilizzino gli accordi di mutua assistenza (MLAT), evitando richieste dirette potenzialmente lesive della sovranità degli Stati membri.

Preoccupazione è stata manifestata dal Gruppo anche in ordine alla proposta di regolamento che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (Etias), presentata dalla Commissione europea a novembre 2016. Con lettera del 10 aprile 2017 (doc. web n. 8668583), il Gruppo, pur riconoscendo la necessità di assicurare un giusto equilibrio tra le esigenze di pubblica sicurezza e il diritto alla protezione dei dati personali, ha richiamato l'attenzione su alcuni aspetti della proposta che suscitano preoccupazioni e sui quali si ritiene necessario intervenire: l'interoperabilità tra i vari sistemi con cui l'Etias sarà collegato o con i quali potrebbe incrociare le informazioni; le procedure manuali poste in essere dalle competenti Unità nazionali in caso di diniego automatico del visto; la necessità di riconoscere un effettivo diritto di appello nel caso di rifiuto dell'autorizzazione di viaggio; i tempi di conservazione dei dati; il trattamento dei dati sensibili relativi allo stato di salute in relazione allo scopo di salvaguardare la salute pubblica (considerato che alcuni dati, in particolare, potrebbero non essere rilevanti per gli scopi del sistema Etias), con un rischio di raccolta non necessaria e sproporzionata; la mancata distinzione tra i differenti scopi che vengono perseguiti.

Trasferimento dati all'estero

In materia di trasferimenti di dati all'estero, il Gruppo ha concentrato la propria attenzione sull'attuazione dell'Accordo EU-USA "Scudo *Privacy*" (*Privacy Shield*) – che è stato oggetto del primo riesame annuale – e sull'aggiornamento, in vista dell'applicazione del RGPD, dei principali documenti precedentemente adottati in tale ambito.

L'Accordo *Privacy Shield*

Come noto, con la decisione (UE) 2016/1250, la Commissione europea ha concluso che gli Stati Uniti d'America assicurano un livello di protezione adeguato dei dati personali trasferiti dall'Unione europea alle organizzazioni statunitensi che si sono autocertificate come aderenti al regime disciplinato dall'Accordo *Privacy Shield*. Il Gruppo ha lavorato al fine di contribuire all'applicazione di tale Accordo, da un lato, mediante l'adozione di due *form* che possono essere utilizzati dagli interessati che intendano presentare un reclamo relativo alla parte commerciale o alla parte "*intelligence & law enforcement*" del *Privacy Shield* (i moduli sono rinvenibili alla pagina del sito dell'autorità dedicata all'Accordo, doc. web n. 5306161) e, dall'altro, mediante l'individuazione delle regole di procedura dei due organismi incaricati di mediare la cooperazione con le autorità statunitensi: il *panel* informale di autorità di protezione dei dati (che è competente a valutare i reclami pervenuti in relazione alla "parte commerciale", doc. web n. 8668708) e quelle dell'organismo centralizzato per l'UE (formato dalle autorità di Bulgaria, Regno Unito, Austria, Germania e Francia, doc. web n. 8668660), incaricato di trasmettere al "Mediatore dello Scudo" i reclami pervenuti in relazione al trattamento da parte di autorità di *intelligence* statunitensi di dati personali trasferiti dall'Unione europea (sia nell'ambito dello Scudo che attraverso l'utilizzo di clausole contrattuali *standard*, *Binding corporate rules* o deroghe).

In settembre, alcuni rappresentanti del Gruppo, in qualità di esperti, hanno incontrato, insieme alla Commissione europea, i rappresentanti delle amministrazioni statunitensi interessate dall'Accordo per lo svolgimento dell'analisi annuale comune sul suo funzionamento. All'esito dell'analisi – che si è incentrata tanto sugli aspetti commerciali di applicazione dell'Accordo quanto su quelli relativi alle eccezioni ai principi per motivi di sicurezza nazionale e di amministrazione della giusti-

zia –, il Gruppo ha adottato un proprio rapporto (che si aggiunge a quello della Commissione europea pubblicato il 18 ottobre 2017) nel quale, nel dare atto degli aspetti positivi, ha evidenziato i rimanenti punti critici (WP 255, doc. web n. 8668611). Per la parte commerciale, in particolare, il parere sottolinea la limitata disponibilità di informazioni rivolte agli interessati, la necessità di aumentare le attività di supervisione (ad es., attraverso *sweep*) e lamenta l'interpretazione differente della nozione di dati relativi al rapporto di lavoro (più restrittiva negli Stati Uniti), la mancata chiara definizione della differente posizione di titolari e responsabili del trattamento, nonché l'assenza in termini generali di disposizioni relative alle decisioni automatizzate. In merito agli aspetti relativi agli accessi da parte di autorità di *intelligence*, il *report* rappresenta la necessità di ottenere conferma che la raccolta di dati per tali finalità non sia indiscriminata e auspica che, prima dell'entrata in vigore del RGPD, il *Privacy and civil liberties oversight board* – PCLOB – venga messo nelle condizioni di poter effettivamente vigilare sulle attività poste in essere (anche attraverso la designazione dei membri mancanti) e che l'*Ombudsperson* (attualmente protempore) venga nominato.

A novembre 2017 sono stati pre-adottati e portati a consultazione pubblica sia il documento di lavoro volto ad aggiornare parte del precedente documento in tema di adeguatezza (WP 12, doc. web n. 1606866) e i due precedenti *referential* relativi agli elementi e ai principi che devono essere contenuti nelle regole vincolanti d'impresa (*Binding corporate rules* - Bcr) per titolari e per responsabili. Alla luce dei commenti ricevuti, il Gruppo ha adottato la versione definitiva dei tre documenti nel febbraio 2018.

Aggiornamento *referential* su adeguatezza e Bcr per titolari e per responsabili

Il *referential* in materia di adeguatezza (WP 254, doc. web n. 8668269) fornisce un quadro aggiornato dei requisiti che un Paese terzo o un'organizzazione internazionale deve rispettare per poter essere considerato "adeguato" ai sensi dell'art. 45 RGPD. Il documento si divide in quattro capitoli: il primo illustra i requisiti generali di adeguatezza; il secondo si sofferma sul ruolo del Comitato europeo per la protezione dei dati in merito alle decisioni sull'adeguatezza; il terzo indica i principi fondamentali e procedurali che devono essere presenti in un Paese terzo/organizzazione internazionale; il quarto ribadisce la necessità che siano garantiti nel Paese terzo il rispetto dei principi di proporzionalità e necessità nel caso di deroghe per finalità di *law enforcement* e sicurezza nazionale.

Il *referential* relativo alle Bcr per titolari (WP 256, doc. web n. 8668319) aggiorna gli elementi che le Bcr devono contenere alla luce del nuovo quadro normativo e, in particolare, introduce nuovi elementi in tema di giurisdizione per la presentazione dei reclami da parte degli interessati (in linea con gli artt. 77 e 79 RGPD); potenzia i requisiti di trasparenza (l'interessato deve essere informato degli elementi di cui agli artt. 13 e 14 del RGPD oltre che dei diritti riconosciutigli quale terzo beneficiario, della clausola relativa alla responsabilità e di quella sui principi di protezione dei dati); amplia la descrizione del campo di applicazione geografico e materiale delle Bcr (struttura e punti di contatto del gruppo e delle sue società, tipi di dati oggetto di trasferimento e categorie di interessati, finalità, ecc.) e allinea i principi di protezione dei dati con quelli previsti dal RGPD (quali liceità, *data retention*, *accountability*, sicurezza – che ora include la necessità di notificare i *data breach* alla capogruppo e al membro UE con delega per la protezione dei dati) nonché gli impegni che le società devono assumersi in relazione alle richieste di accesso ai dati da parte di autorità pubbliche di Paesi terzi.

Il *referential* per le Bcr per responsabili (WP 257, doc. web n. 8668378) contiene nuovi elementi che rispecchiano quelli introdotti nelle Bcr for *controller* e aggiungono alcuni punti alla luce delle peculiarità del ruolo dei "*processor*". In particolare,

le novità specifiche riguardano i diritti dei terzi beneficiari (tra cui ora i diritti che possono essere esercitati direttamente nei confronti del *processor* in relazione agli obblighi che il RGPD pone loro in capo: cfr. artt. 28, 29 e 79 RGPD) e l'accordo di servizio tra titolare del trattamento e responsabile (che deve contenere gli stessi elementi previsti dall'art. 28 RGPD).

Entrambi i documenti spiegano che le Bcr già adottate nell'ambito della procedura europea di cooperazione (e mutuo riconoscimento) possono continuare ad essere utilizzate dai gruppi, senza dover passare per una nuova procedura di adozione ai sensi dell'art. 64 del RGPD, se le stesse verranno "aggiornate" alla luce delle nuove disposizioni del RGPD e dei nuovi *referential*.

Bcr per titolari e Bcr per responsabili

Sempre in tema di Bcr, è proseguita la cooperazione tra le autorità di protezione dei dati europee per l'adozione "comune" a livello europeo di Bcr che, ove previsto dalle normative nazionali, devono essere poi autorizzate dalle diverse autorità dei Paesi da cui i dati vengono trasferiti. Nel 2017 sono state avviate 25 procedure per l'approvazione di Bcr per titolari e 15 per Bcr per responsabili e sono state concluse, con il riconoscimento dell'adeguatezza delle clausole nelle stesse contenute, 10 Bcr per titolari e 5 Bcr per responsabili.

In 8 procedure il Garante partecipa in qualità *co-reviewer* al fine di rendere conformi al quadro normativo europeo i testi delle Bcr proposte dai gruppi (per le autorizzazioni nazionali rilasciate dal Garante si fa rinvio al cap. 17).

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

Europol: l'attività dell'Autorità di controllo comune (ACC)

A seguito del nuovo quadro normativo creato dal regolamento (UE) 2016/794 che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol), entrato in vigore il 1° maggio 2017, l'ACC Europol ha cessato il proprio mandato ad aprile 2017. La supervisione sull'attività svolta da Europol ai sensi del regolamento suddetto è stata affidata al Garante europeo per la protezione dei dati (Gepd), inclusa l'attività ispettiva, ed è stato istituito un Consiglio di cooperazione (*Europol Cooperation Board*) per assicurare una stretta cooperazione con le autorità competenti sulla vigilanza della legittimità della comunicazione di dati ad Europol e garantire i diritti degli interessati. Al fine di assicurare la transizione delle attività di supervisione tra l'ACC Europol e il Gepd, il segretariato dell'ACC e quello del Gepd hanno svolto un'intensa attività volta alla formazione dei nuovi supervisori ed alla selezione e messa a disposizione della rilevante esperienza (e documentazione) acquisita dall'ACC anche nel corso delle numerose ispezioni svolte dalla sua istituzione. L'ACC Europol, sotto la presidenza del rappresentante italiano, dott.ssa Vanna Palumbo, ha tenuto l'ultima riunione il 19 aprile 2017, nel corso della quale ha adottato il sesto (ed ultimo) rapporto di attività, che copre le ultime attività svolte (novembre 2012-aprile 2017, doc. web n. 8645298). Ha inoltre completato la discussione sulla proposta di regolamento interno del Consiglio di cooperazione, redigendo e votando un testo da presentare in occasione della prima riunione del nuovo consesso in modo da consentire a questo di poter, approvandolo, entrare subito nella pienezza dei poteri e procedere all'elezione degli organi rappresentativi. È stato anche presentato il rapporto dell'ultima ispezione, svolta nel gennaio 2017, che ha avuto come oggetto la verifica dell'attuazione delle prescrizioni finora impartite dall'ACC, da cui è emerso un buon livello di adempimento. L'ACC ha senz'altro rappresentato un'esperienza di successo nel campo della protezione dei dati; ha tenuto 81 riunioni (52 il Comitato ricor-

si), svolto 24 ispezioni e 52 verifiche in relazione a richieste presentate dagli interessati.

Il Consiglio di cooperazione di Europol (Europol CB) ha funzioni consultive (adozione di pareri, linee guida, raccomandazioni e buone prassi; cfr. l'art. 45 del regolamento (UE) 2016/794), è composto da un rappresentante di un'autorità di controllo nazionale di ciascuno Stato membro e dal Gepd e dispone del supporto di un segretariato dedicato, fornito dal Gepd. La prima riunione del Consiglio si è tenuta il 14 giugno 2017, sotto la presidenza del rappresentante del Gepd. Nel corso della stessa, il Consiglio ha adottato il regolamento interno elaborato dall'ACC Europol, apportando alcune modifiche; ha eletto il Presidente (Francois Pellegrini, componente della Cnil - FRA) e il Vice (Gabriele Lownau, dell'ufficio del Garante federale tedesco - GER). La seconda riunione del Consiglio si è svolta il 16 novembre 2017 e la discussione ha riguardato anche l'aggiornamento del regolamento 45/2001 e la posizione assunta al riguardo dal Parlamento europeo, attesa la criticità concernente la volontà di quest'ultimo di trovare una soluzione unica per il regime di protezione dei dati e per la relativa modalità di supervisione, che non tiene conto della specialità del vigente regolamento Europol e che porta a far prevalere le disposizioni del regolamento 45/2001 su quelle dei regolamenti specifici per tutti i trattamenti di dati svolti, non solo in relazione alle attività di tipo amministrativo ma anche a quelle operative. Considerato che ciò ha un notevole impatto in quanto amplia ulteriormente i poteri e il ruolo del Gepd, limitando la necessaria cooperazione con le Autorità nazionali di protezione dei dati, si è dato mandato al Presidente di predisporre con urgenza una lettera da adottare con procedura scritta e trasmettere ai co-legislatori per intervenire prima della conclusione del trilogo. La lettera è stata adottata ed inviata nel mese di dicembre (doc. web n. 8641955). Il Consiglio ha preparato la prima ispezione da effettuare ad Europol congiuntamente con il Gepd decidendo di avvalersi delle competenze già possedute in merito dai componenti del *team* d'ispezione operante presso l'ACC Europol e ha considerato positivamente la richiesta fatta dal Presidente dell'ACC Europol nella lettera di chiusura dell'attività di quest'organo, di dare continuità ad alcune attività intraprese, in particolare aggiornando l'opuscolo sui diritti dell'interessato, il manuale per le unità nazionali Europol (UNE/ENU), e di seguire le raccomandazioni contenute nel rapporto sulle vittime del traffico di esseri umani.

La prossima riunione del Consiglio è prevista nella primavera del 2018.

Il Sistema Informativo Schengen: l'attività del Gruppo di coordinamento della supervisione SIS II

Nell'ambito del Sistema Informativo Schengen (v. sopra par. 7.6), il Gruppo si è riunito due volte nel 2017 e, terminato il periodo di presidenza dalla portoghese Clara Guerra, ha eletto presidente il maltese David Cauchi. Nel corso delle riunioni è stata discussa la nuova proposta di regolamento sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale (COM(2016) 883 *final*) presentata dalla Commissione che aggiornerà la normativa relativa al SIS II ed è stato inoltre illustrato il parere adottato al riguardo dal Gepd il 3 maggio 2017 (pubblicato su GUCE C 200/14 del 23 giugno 2017). In particolare, sono state manifestate preoccupazioni in ordine alla mancanza di una valutazione d'impatto adeguata in materia di: inserimento, oltre che delle impronte digitali, anche del riconoscimento del palmo tra le funzionalità in base alle quali ricercare dati nel sistema; allargamento dell'accesso al sistema ad organismi UE, la cui competenza non è ben definita (FRONTEX); estensione da tre a cinque anni del periodo di conservazione generale delle segnalazioni relative a persone. Tali criticità sono state rappresentate con una lettera inviata dalla Presidente al Parlamento europeo (doc. web n. 8645578).

22

Una lettera è stata inviata inoltre alle istituzioni dell'UE per richiedere che sia assicurato un adeguato finanziamento delle Autorità nazionali in relazione ai nuovi compiti assegnati (doc. web n. 8641869) e nella riunione del novembre 2017 è stato dato atto della risposta fornita dalla Commissione europea (commissario Avramoupolos) al riguardo (doc. web n. 8645388).

Alla luce delle informazioni raccolte attraverso un questionario inviato alle autorità nazionali competenti in materia di accesso ai dati contenuti nel sistema, il Gruppo ha adottato un rapporto volto a fornire una panoramica del modo in cui il SIS II viene attuato in pratica a livello nazionale al fine di identificare e attuare nuove azioni per il gruppo e i suoi membri (doc. web n. 8668767).

Il Gruppo sta ancora lavorando ad un catalogo delle raccomandazioni formulate a seguito delle valutazioni Schengen nel settore della protezione dei dati personali nei diversi Paesi e sugli esiti di un questionario volto ad acquisire informazioni sulla politica di registrazione degli accessi (*logging*) seguita a livello nazionale.

Gruppo di supervisione Eurodac

Il Gruppo si è riunito due volte nel corso del 2017. La Commissione e l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (EU-LISA) hanno informato sulle attività in corso. Dalle informazioni fornite da EU-LISA è emerso un problema relativo alla qualità delle impronte rispetto al nuovo *standard* richiesto, che rende più alto il livello di errore, con possibili falsi *hits*. Al riguardo, un progetto pilota (che vede la partecipazione di EU-LISA e gli Stati membri interessati) prevede l'utilizzo di una differente tecnologia, che consentirebbe di rilevare le impronte digitali garantendo un'elevata qualità anche in presenza di mutilazioni. Nel corso delle predette riunioni la Commissione ha fornito informazioni sullo stato della nuova riformulazione (*recast*) del regolamento Eurodac, in merito al quale il Parlamento europeo ha adottato nel giugno 2017 la sua posizione ai fini del negoziato sul testo.

Tra i temi discussi nel corso delle riunioni del Gruppo e da affrontare in futuro, figurano: la cancellazione anticipata dal sistema, le ricerche "speciali" (che riguardano l'esercizio dei diritti di accesso da parte delle persone segnalate nel sistema) ed eventuali problematiche emergenti dall'accesso ad Eurodac da parte delle forze dell'ordine, considerato che dai rapporti e dalle statistiche presentate da parte di EU-LISA e della Commissione emerge che solo alcuni Stati membri sembrerebbero interessati (in proposito, si è chiesto alle varie autorità di svolgere le opportune verifiche a livello nazionale).

Il Sistema informativo visti (VIS): Gruppo di coordinamento della supervisione

Il Gruppo si è riunito due volte nel corso del 2017. Nel corso di tali riunioni si è discusso della definitiva adozione delle proposte legislative per l'introduzione di un sistema di entrata/uscita (EES), di un sistema di autorizzazione preventiva all'entrata nel territorio EU (ETIAS), degli strumenti destinati a meglio disciplinare i rimpatri, quali le modifiche al regolamento SIS II ed Eurodac. La Commissione ha inoltre menzionato i risultati della valutazione complessiva pubblicata nell'ottobre 2016 sul funzionamento del VIS, svolta in attuazione del regolamento 767/2008 (REFIT) e delle conclusioni, in base alle quali è previsto che la Commissione conduca una valutazione d'impatto per analizzare e definire le diverse opzioni di modifica dell'attuale quadro legislativo. Nella comunicazione del marzo 2017, sempre in tema di rimpatri, si ipotizza uno studio per valutare la possibilità di inserire nel VIS una copia dei documenti di viaggio per facilitare l'identificazione dei migranti irregolari.

È proseguito il lavoro del sottogruppo incaricato di valutare la coerenza delle attuali pratiche in materia di esternalizzazione a società private della gestione delle procedure per la presentazione delle domande di visto, inclusa l'acquisizione delle

impronte digitali dei richiedenti. Al riguardo, tenendo presente quanto emerso dalla predetta valutazione svolta dalla Commissione nonché le raccomandazioni rivolte dai *team* di esperti che hanno svolto le valutazioni nei Paesi Schengen fin qui visitati, sono state identificate alcune questioni chiave per individuare future buone prassi da suggerire alle autorità competenti. Il rapporto predisposto sarà approvato con procedura scritta in modo da completare l'attività così come il rapporto sull'applicazione dell'art. 41. È stato completato il rapporto biennale di attività per gli anni 2015 e 2016, essendo pervenuti tutti i contributi nazionali, il cui testo dopo l'adozione è stato formalmente trasmesso al Consiglio dell'UE (doc. web n. 8645508). Per il posto di presidente la svizzera Caroline Gloor Scheidegger è succeduta alla dr.ssa Vanna Palumbo del Garante. Il Gruppo si riunirà nuovamente nella tarda primavera del 2018.

Il Sistema informativo doganale (SID): ACC Dogane e Gruppo di coordinamento della supervisione SID

L'ACC Dogane (competente per la supervisione del Sistema informativo doganale sulla base della decisione 2009/917/GAI e della decisione quadro 2008/977/GAI in relazione ai trattamenti effettuati per facilitare la prevenzione, la ricerca e il perseguimento di gravi infrazioni alle leggi nazionali) e il Gruppo di coordinamento della supervisione del Sistema informativo doganale (che svolge la propria attività di supervisione del sistema informativo utilizzato, sulla base del regolamento (EC) n. 515/1997, consolidato nel 2008, per contrastare le violazioni di natura amministrativa) si sono riunite nell'aprile 2017, proseguendo le diverse attività pianificate e le attività di *follow-up*. In particolare, il Gruppo ha adottato il programma di lavoro per il 2017-2018 (doc. web n. 8642107) e ha proseguito i lavori su modelli comuni per le ispezioni nazionali del SID. Come attività di *follow-up*, il Gruppo ha deciso di verificare in che modo i diritti degli interessati siano rispettati a livello nazionale e dell'UE anche alla luce della guida all'accesso al CIS, adottata a dicembre 2015 (doc. web n. 4810368).

22.3. *Le conferenze delle Autorità su scala internazionale*

La Conferenza internazionale delle Autorità di protezione dati

Si è tenuta ad Hong Kong dal 25 al 29 settembre la 39ª Conferenza internazionale delle Autorità di protezione dei dati. Nel corso dei lavori, ai quali ha partecipato una rappresentanza del Garante, sono stati affrontati temi cruciali del mondo iperconnesso legati all'intelligenza artificiale, alla *cybersecurity*, ai trasferimenti transfrontalieri di dati, alle differenze delle legislazioni in materia di *privacy* e alla necessità di individuare "denominatori comuni".

Nel corso della sessione a porte chiuse della Conferenza è stato affrontato il tema dello scambio di informazioni nel settore pubblico e dell'utilizzo delle informazioni conservate in *database* pubblici da parte dei governi. Questi dati sono necessari, infatti, per guidare l'innovazione commerciale, diffondere la conoscenza, aumentare la trasparenza, migliorare i servizi pubblici e ottenere risparmi sui costi e efficienza. Se tali utilizzi possono da un lato produrre risultati positivi per gli individui, gli stessi rischiano dall'altro di favorire intrusioni indebite nella vita privata.

Sono state adottate le tre risoluzioni presentate alla Conferenza: una sul tema delle *connected cars* – per la quale il Garante è stato *co-sponsor*, tenuto anche conto del lavoro fatto dall'Autorità in tale ambito in seno al WP 29 (v. *supra*) –, una sulla collaborazione tra autorità di protezione dati e autorità di tutela dei consumatori nell'economia digitale ed una sul tema della cooperazione internazionale tra autorità di protezione dei dati. L'obiettivo di quest'ultima risoluzione è rivedere e integrare il lavoro già svolto in materia, in particolare in occasione della 36ª Conferenza tenu-

tasi a Mauritius dove venne approvato il *Global cross border enforcement cooperation "arrangement*". Con l'adozione della risoluzione, l'Accordo, che aveva lo scopo di favorire la cooperazione tra le "*Privacy enforcement authority*", sottoscritto da alcune Autorità di protezione dei dati europee, è stato modificato con l'introduzione di un allegato relativo alle salvaguardie che devono essere garantite nello scambio di dati personali a fini di cooperazione. Viene inoltre rafforzato il ruolo del Comitato esecutivo della Conferenza internazionale che avrà, tra l'altro, il compito di ricevere le dichiarazioni di intenti delle autorità che intendono partecipare, rivederle e raccomandare alla Conferenza internazionale la sospensione o l'esclusione dall'Accordo di autorità che non lo abbiano rispettato.

La Conferenza delle Autorità europee *(Spring Conference)*

Le Autorità europee di protezione dei dati si sono riunite a Limassol (Cipro) il 27-28 aprile, con la partecipazione del Garante al *panel* sulla sensibilizzazione del pubblico sulla protezione dei dati e sulla necessità di favorire il dialogo delle Autorità di protezione dei dati con la collettività e le realtà imprenditoriali. All'esito della Conferenza è stata adottata una risoluzione con la quale le Autorità hanno rimarcato la necessità di portare a termine il processo di modernizzazione della Convenzione n. 108/1981 del Consiglio d'Europa, invitando i governi europei a raggiungere al più presto un accordo politico per una rapida finalizzazione della nuova Convezione 108. Sono state adottate le regole procedurali sul funzionamento della Conferenza, inclusi i criteri per l'accreditamento delle autorità e per l'ottenimento dello *status* di osservatori. È stato altresì discusso il tema del ruolo della Conferenza e della sua direzione strategica. A tal proposito, su proposta della presidente del Gruppo Art. 29, la Conferenza ha deciso di istituire un Gruppo di lavoro per esaminare tali tematiche.

22.4. *La partecipazione ad altri comitati e gruppi di lavoro internazionali*

T-PD

È proseguita e si è anzi intensificata l'attività all'interno del Comitato consultivo della Convenzione n. 108/1981 (cd. T-PD, anche nella sua composizione ristretta, cd. T-PD *Bureau*) del quale il Garante, dalla plenaria del 29 giugno -1° luglio 2016, ha assunto la presidenza.

Linee guida in materia di *big data*

Il lavoro di approfondimento in materia di *big data* (v. Relazione 2016, p. 161) si è concluso con l'adozione, all'esito di procedura scritta terminata il 23 gennaio 2017, di specifiche linee guida (doc. web n. 6108739). Il testo – che pur essendo basato sulla Convenzione n. 108 si ispira ai principi contenuti nella versione modernizzata della stessa (v. *infra*) – si rivolge a titolari e responsabili del trattamento e ai legislatori nazionali evidenziando i principi di protezione dati cui adempiere affinché i benefici derivanti dall'impiego di *big data* possano essere perseguiti nel rispetto dei diritti della persona.

Le linee guida insistono sulla necessità di non avvalersi esclusivamente degli strumenti tradizionali a disposizione dell'interessato per il controllo sui propri dati quali informativa e consenso, quanto piuttosto di predisporre preventivi meccanismi di valutazione dell'impatto di *big data* sui diritti della persona, compresa la dimensione etica di tali ripercussioni, nonché di adottare adeguate soluzioni di *privacy by design* nelle diverse fasi del trattamento fin dal suo inizio. Sottolineano inoltre la necessità di preservare l'autonomia dell'intervento umano nelle decisioni automatizzate fondate su *big data*, di garantire l'accesso dell'interessato alla logica del trattamento che lo riguarda, incluse le conseguenze che da esso derivano nonché di contestare le decisioni fondate su tali trattamenti e di prestare adeguate garanzie

per evitare i rischi di discriminazione che possono derivare dagli automatismi di un processo decisionale spesso oscuro.

Le linee guida costituiscono un primo contributo del Comitato in materia di *big data* e potranno essere seguite da ulteriori interventi nei diversi settori interessati.

Guida pratica sul trattamento dei dati in ambito di polizia

È proseguito il lavoro del Comitato sul trattamento dei dati in ambito di polizia, sfociato nell'adozione, in procedura scritta il 15 febbraio 2018 (doc. web n. 8645776), di una guida pratica sull'impiego dei dati personali da parte degli operatori del settore.

La Guida – che riconosce la centralità del trattamento dei dati personali nel contrasto delle attività criminose – mira a fornire *best practices* affinché l'impiego di dati personali in ambito di polizia avvenga nel rispetto dei principi della Convenzione n. 108 e della raccomandazione (87)15, che rimane tuttora il testo giuridico base del Consiglio d'Europa per la protezione dei dati in tale settore.

Il documento fornisce indicazioni, anche ricorrendo all'esemplificazione, su come rispettare il principio di legalità del trattamento, la legittimità e proporzionalità nella raccolta delle informazioni e nei loro ulteriori compatibili impieghi, sulle salvaguardie addizionali che devono essere garantite ove il trattamento riguardi categorie di dati sensibili, sull'impiego di meccanismi di valutazione preventiva circa l'impatto del trattamento, nonché sugli obblighi di trasparenza e i diritti degli interessati, seppur con le eccezioni e limitazioni necessarie a non compromettere le esigenze di investigazione.

La guida si sofferma inoltre sull'impiego di nuove tecnologie nel settore della polizia, in particolare con riferimento alla internet delle cose e *big data*, prevedendo anche in questo caso specifiche cautele volte a determinare preventivamente le conseguenze dell'uso di tali nuove tecnologie sui diritti delle persone, in particolare attraverso il *data protection impact assessment*, e l'introduzione di meccanismi di *privacy by design*.

Raccomandazione in materia di dati relativi alla salute

È proseguito il lavoro del Comitato sulla revisione della raccomandazione (97)5 sulla protezione dei dati relativi alla salute. La modernizzazione del testo del 1997 si è resa necessaria per la diffusione in ambito sanitario di nuove tecnologie che hanno notevolmente modificato lo scenario originario e richiesto l'approntamento di garanzie adeguate.

La nuova bozza di raccomandazione si fonda sulla nozione di "dati relativi alla salute" (più ampia di quella originaria di "dati sanitari") che comprende i dati personali relativi alla salute mentale o fisica di un individuo, compresi quelli che riguardano la fornitura di servizi di cura, che rivelano informazioni sulla salute passata, presente e futura, della persona.

Il testo si sofferma sulle necessarie basi giuridiche su cui deve fondarsi il trattamento di tale categoria speciale di dati, la cui protezione, in base all'art. 6 della Convenzione n. 108, appare "rafforzata" per il potenziale discriminatorio derivante dal loro uso. Contiene specifiche garanzie che devono assistere il trattamento di dati genetici, categoria "super sensibile" per il carattere predittivo che li contraddistingue, e fornisce indicazioni sulla condivisione dei dati personali di pazienti da parte di più professionisti per garantire una migliore assistenza medica. La bozza si sofferma altresì sul trattamento in ambito di ricerca scientifica affinché questa possa essere effettuata nel rispetto dei principi di trasparenza e di adeguate garanzie, tra cui il consenso dell'interessato. Offre infine chiarimenti sui requisiti che i dispositivi interoperabili sempre più diffusi nella sanità devono rispettare per garantire la sicurezza e confidenzialità delle informazioni trasmesse nonché sui principi di protezione dati che devono essere assicurati nell'impiego e nella configurazione di applicazioni mobili.

22

ICANN

Il T-PD ha lavorato al progetto di raccomandazione in stretto contatto con il Comitato del Consiglio d'Europa DH-BIO competente sulle questioni di bioetica, per gli evidenti punti di contatto tra le materie seguite dai due comitati e per garantire coerenza tra i diversi strumenti emanati dal Consiglio d'Europa.

Il Comitato ha inoltre proseguito la sua attività di approfondimento sulle questioni relative al trattamento di dati nell'ambito di Icann, in particolare con riferimento ai principi di protezione dati che devono applicarsi anche al cd. registro *Whois*. Il Comitato ha preso parte all'incontro di Icann (Copenaghen, 11-16 marzo), in particolare nella sessione centrale della riunione concernente il rispetto dei diritti umani.

Modernizzazione della Convenzione n. 108

Il Comitato – pur avendo terminato il lavoro tecnico sulla modernizzazione della Convenzione n. 108 (era stato infatti il T-PD ad adottare nel 2012 il documento di lavoro che ha costituito la base della discussione in seno al Comitato *ad hoc* CAHDATA, v. Relazione 2016, p. 160) – ha comunque continuato a seguire i lavori della revisione, nel frattempo passati alla competenza del Comitato dei ministri, chiamato a sciogliere i nodi ancora irrisolti del processo, in particolare sul trasferimento dei dati verso paesi terzi, sul diritto di voto dell'UE nelle decisioni del Comitato, sulle eccezioni che gli Stati membri possono apportare ai principi della Convenzione specie nell'ambito della sicurezza nazionale e sulle procedure per l'adozione del protocollo emendativo della Convenzione.

Nuove adesioni alla Convenzione n. 108

È crescente intanto l'attenzione da parte di Stati, anche al di fuori del Consiglio d'Europa, nei confronti della Convenzione n. 108/1981, che rimane a tutt'oggi il solo strumento giuridicamente vincolante a livello internazionale sulla protezione dei dati.

Il Comitato dei Ministri del Consiglio d'Europa, rispettivamente nelle riunioni del 22-23 Marzo e del 27 settembre 2017, ha dato il proprio assenso alla richiesta del Burkina Faso e dell'Argentina per ottenere l'invito ad accedere alla Convenzione n. 108 su cui anche il T-PD si era espresso a favore con i pareri del 7 febbraio 2017 (T-PD(2016)21, doc. web n. 8645700) e del 29 agosto 2017 (T-PD(2017)12, doc. web n. 8645737).

Salgono così a otto i paesi non membri del Consiglio d'Europa invitati all'accessione dopo Uruguay, Marocco, Mauritius, Senegal, Tunisia (ormai divenuti Parti) e Capo Verde (in corso di adesione).

Il T-PD ha inoltre dato parere positivo alla richiesta da parte del Messico di accedere alla Convenzione n. 108 (T-PD(2017)17, doc. web n. 8785066).

Nel corso dell'anno hanno inoltre richiesto e ottenuto lo status di osservatore presso il Comitato il Giappone, Israele, Repubblica di Corea, Repubblica delle Filippine, il Consiglio per la Trasparenza del Cile, l'autorità di protezione dei dati della Repubblica del Ghana e il *Privacy Commissioner* della Nuova Zelanda.

Comitato *ad hoc* per i diritti dei minori (CAHENF)

Il Garante ha partecipato al Gruppo di lavoro di esperti sui minori e l'ambiente digitale nell'ambito del Comitato *ad hoc* per i diritti dei minori (CAHENF) del Consiglio d'Europa. Il gruppo di lavoro (CAHENF-IT) è stato istituito allo scopo di redigere uno schema di linee guida sull'accesso sicuro dei minori al web e sulla loro tutela nell'ambiente digitale, da sottoporre al CAHENF, in vista dell'adozione di una apposita raccomandazione da parte del Comitato dei Ministri del Consiglio d'Europa.

La bozza di linee guida, che muove dai diritti dei minori riconosciuti da diversi strumenti internazionali ed elaborati dalla giurisprudenza della Corte europea dei diritti dell'uomo, intende guidare gli Stati membri nella formulazione di adeguate *policy* volte a proteggere ed attuare i diritti dell'infanzia nel mondo digitale, assicurare che gli attori coinvolti, i fornitori di servizi via internet e, più in generale, di

servizi digitali, si facciano carico delle responsabilità nella tutela dei minori e della promozione di azioni concertate a livello internazionale per il raggiungimento di tali obiettivi.

Parte importante delle linee-guida è dedicata alla tutela della vita privata e della protezione dei dati in ambito digitale. In particolare il documento si sofferma sulla necessità di assicurare che il trattamento dei dati sia basato su un'adeguata base giuridica, ad esempio il consenso informato del minore o di chi esercita la responsabilità genitoriale, sull'opportunità – nel processo di individuazione dell'età congrua per la prestazione del consenso – di tenere conto delle capacità di comprensione del minore nei diversi stadi della sua crescita e di fornire informative adeguate, di prestare particolare attenzione ai rischi derivanti dalla profilazione, anche attraverso l'impiego di *smart toys*.

OCSE - WPSPDE

L'Autorità ha continuato a partecipare ai lavori del WPSPDE (*Working party on security and privacy in digital economy* già *Working party on information security and privacy*) dell'OCSE, anche nella sua composizione ristretta. Il Garante, già membro del Gruppo e componente del *bureau* del WPSPDE, ha lavorato in prima linea nell'incarico di vicepresidenza del Gruppo per il 2017 partecipando alle due riunioni plenarie (maggio/ottobre) e relative riunioni del *bureau*, nonché a diverse *conference call* e a due *workshop* tematici.

Nel corso dell'anno è stato ultimato il lavoro sul DEO (*Digital economy outlook*, pubblicazione di punta di punta biennale del Comitato CDEP) e sono stati presentati i risultati relativi alle sezioni relative alla sicurezza e alla *privacy* del questionario DEO, nonché ai capitoli relativi al rischio digitale, la fiducia e gli sviluppi di politiche di settore. Notevoli progressi si sono registrati anche in relazione al lavoro sulla revisione della raccomandazione OCSE sulla protezione delle infrastrutture critiche (raccomandazione CIIP del 2008), confermando l'intenzione di chiudere il lavoro di aggiornamento entro il 2019. Il Gruppo ha altresì elaborato e presentato nella Plenaria di ottobre il *report* con i risultati del questionario sulle implicazioni del lavoro della revisione in corso della raccomandazione OCSE sulla protezione dei minori *online*, adottata dal Consiglio OCSE nel 2012, in relazione alla quale è stata avanzata la proposta di un *workshop* sulla "Protezione dei minori in un Mondo Connesso" da tenersi nel corso del 2018. Sempre nel corso della plenaria di ottobre la *Health Division* ed il Segretariato del WPSPDE hanno presentato la bozza della guida per l'attuazione della raccomandazione OCSE sui dati relativi alla salute adottata nel 2016 (v. Relazione 2016, p. 163).

Enhanced access to data

Nel primo semestre dell'anno il Gruppo ha lavorato intensamente sulla valorizzazione dell'accesso ai dati per favorire l'innovazione digitale. In particolare, si è tenuto in Danimarca (2-3 ottobre) un *workshop* dedicato al tema del *Enhanced access to data*. Si è trattato del primo *workshop* del Progetto sull'accesso rafforzato ai dati (OECD *Expert workshop on "Enhanced access to data: reconciling risks and benefits of data reuse*"), co-sponsorizzato da Danimarca, Finlandia, Italia, Giappone, Norvegia e Svezia. Tale *workshop* ha affrontato questioni fondamentali di *governance* dei dati, quali l'interoperabilità dei dati e il diritto alla portabilità degli stessi, la proprietà, il controllo e la qualità dei dati nonché il loro valore e *pricing*. Dalla discussione è emersa la necessità condivisa di un dialogo e di una cooperazione internazionale sul tema della *Data driven innovation* (DDI) al fine di orientare i decisori politici dei Paesi OCSE verso un adeguato bilanciamento tra DDI e *data protection*, massimizzando i benefici sociali ed economici del riuso dei dati e dell'innovazione guidata dai dati e allo stesso tempo affrontando le legittime preoccupazioni dei consumatori e dell'industria. Sulla base dei risultati di questo primo *workshop*, un secondo *workstream* nel 2018 avrà lo scopo di svi-

22

Sviluppo della misurazione degli incidenti di sicurezza digitale e gestione del rischio

luppare i principi generali sull'accesso rafforzato ai dati. Essi potrebbero confluire in una futura raccomandazione del Consiglio OCSE, tema del quale il Garante continuerà ad occuparsi, anche nel contesto del *Joint steering group* (JSG) che lavora di concerto con gli altri due comitati OCSE interessati a tale materia (CSTP e PGC).

Si è tenuto a Zurigo presso il *Swiss re centre for global dialogue* (12-13 maggio) un *workshop* dedicato ad altro importante tema su cui il WPSPDE ha lavorato nel 2017, ossia lo sviluppo della misurazione degli incidenti di sicurezza digitale e gestione del rischio (*Improving the measurement of digital security incidents and risk management*). Il *workshop* ha confermato l'importanza, tra l'altro, del *data sharing* e fornito l'occasione per fare il punto delle iniziative intraprese nei vari Paesi OCSE volte a favorire lo sviluppo di *data set* più affidabili al fine di ovviare incidenti di sicurezza digitali, promuovendo l'adozione delle migliori pratiche di sicurezza digitale e di gestione del cd. rischio *privacy*.

IWGDPT

L'Autorità ha proseguito la sua partecipazione all'*International Working Group on Data Protection in Telecommunication* (IWGDPT) che nel 2017 si è riunito a Washington il 24-25 aprile ed a Parigi il 27-28 novembre.

Tra i principali temi affrontati, si segnala quello del trattamento dei dati per finalità di *intelligence* (doc. web n. 8642234). Il tema – già oggetto di un primo documento di lavoro del Gruppo nel 2013 (cfr. Relazione 2013, p. 187) – continua a destare particolare apprensione e il Gruppo richiama l'attenzione sulla necessità di adottare una nuova serie di principi internazionali volti a rafforzare la supervisione delle agenzie di *intelligence* e delle informazioni dalle stesse raccolte. Ruolo importante dovrebbe essere riconosciuto, secondo il Gruppo, alle autorità di protezione dei dati che dovrebbero intervenire nel dibattito al fine di promuovere il rispetto dei principi di liceità del trattamento, proporzionalità e necessità e qualità nel trattamento dei dati, la trasparenza dei processi e chiare regole di supervisione.

Il Gruppo ha altresì adottato un documento di lavoro sulle piattaforme *e-learning* (doc. web n. 8645088) che, sempre più utilizzate, consentono di raccogliere numerosi dati personali relativi a studenti e ai loro comportamenti. Il documento richiama l'attenzione sui rischi che tali raccolte di dati possono comportare se utilizzate, ad esempio, per finalità diverse da quelle legate all'*e-learning* quali le finalità di *marketing* o per prendere decisioni in ordine alla persona alla quale si riferiscono (ad es., in ambito lavorativo o per la concessione di un affitto o di un credito). Numerose raccomandazioni vengono quindi rivolte alle istituzioni scolastiche per un uso di tali piattaforme conforme alle discipline di protezione dei dati (ad es., in materia di informativa da fornire a genitori e studenti, trasparenza degli algoritmi utilizzati, periodi congrui per la conservazione dei dati, possibilità di esercitare i diritti di rettifica e cancellazione dei dati).

A novembre il Gruppo ha adottato un parere sul trattamento dei dati effettuato nell'ambito del registro *Whois* gestito da Icann (doc. web n. 8645213) nel quale, nell'evidenziare gli aspetti che destano preoccupazione, sono fornite alcune raccomandazioni circa la necessità di adottare idonee misure per rispettare i principi di liceità, finalità del trattamento e di minimizzazione dei dati trattati, in particolare attraverso l'adozione di un approccio multilivello (che renda pubblici solo i dati necessari) e l'applicazione di una *policy* di *data retention* dei dati dei *registrant*. Il Gruppo richiama inoltre Icann al rispetto delle regole per il trasferimento dei dati dall'Unione europea all'estero.

L'*Internet of Things* (IoT) ha formato oggetto di discussione in occasione dell'adozione di un documento di lavoro in materia di aggiornamento del *software* di

base per il funzionamento dei dispositivi IoT (doc. web n. 8645153). Il tema è in questo caso legato alla natura proprietaria del *software* e alla miniaturizzazione, fattori che impediscono spesso un regolare aggiornamento del dispositivo (ad es., per limiti sulla durata della carica delle batterie di alimentazione), esponendolo a malfunzionamenti o ad attacchi di sicurezza. Il documento raccomanda il ricorso a procedure standardizzate di *upgrade* software (anche mediante certificazioni) e l'integrazione dei dispositivi miniaturizzati con altri dispositivi, come *smartphone*, *tablet*, PC, dotati di *display* con cui meglio possono essere esercitati i diritti, *in primis* di trasparenza, degli interessati. Anche gli utenti devono essere parte di un ciclo di vita virtuoso del dispositivo, con un atteggiamento più consapevole sugli aspetti di sicurezza, che deve essere incentivato attraverso azioni informative efficaci e ripetute da parte dei produttori.

Cipl

Si è tenuto a Madrid (6 e 7 marzo) il terzo *workshop* sul RGPD organizzato dal *think tank* Cipl (*Centre for information policy leadership*) e co-ospitato dalla Autorità per la protezione dei dati spagnola (v. Relazione 2016, p. 165). Il Garante vi ha partecipato unitamente a delegati delle altre Autorità europee per la protezione dei dati, al Gepd, alla Commissione europea e ad esperti di Ministeri nazionali e rappresentanti dell'industria. Si è discusso, tra l'altro, del *memorandum discussion paper* elaborato dal Cipl contenente raccomandazioni preliminari su come applicare e attuare le prescrizioni del RGPD in materia di trasparenza, consenso e interesse legittimo. Si è al riguardo condivisa la necessità di esplorare ulteriormente diverse questioni aperte che il Cipl ha poi messo a sistema in due *paper di follow up* del *workshop*. In particolare il Gruppo ha preparato un *white paper* su trasparenza e uno su consenso e interesse legittimo in base al contenuto del citato *memorandum* e agli *input* aggiuntivi raccolti durante il *workshop*. Il *workshop* ha rappresentato anche l'occasione per raccogliere le opinioni dei rappresentanti dell'industria europea sullo stato di avanzamento del regolamento e per svolgere un giro di tavolo in cui i rappresentanti delle Autorità europee per la protezione dei dati e dei Governi hanno illustrato lo stato dell'arte sull'implementazione nazionale del regolamento.

Progetto CRISP

Nel corso del 2017 il Garante ha proseguito la partecipazione al progetto CRISP *(Evaluation and certification schemes for security products*) in particolare collaborando alla stesura del documento CEN *workshop agreement* (CWA) "*Guidelines for the evaluation of installed security systems, based on S-T-E-Fi criteria*" contenente la metodologia CRISP che considera, quali dimensioni per la valutazione di un prodotto/sistema di sicurezza, oltre alla *security* dei prodotti/sistemi, anche la fiducia (*trust*) degli utenti, l'*efficiency* economica e il *freedom infringement*, ovvero l'impatto sulle libertà e diritti individuali, fra i quali quello alla protezione dei dati (STEFi *dimensions*). A seguito dei perfezionamenti effettuati durante e a valle dell'incontro del 16 gennaio 2017 presso la sede del CEN, il CWA è stato sottoposto a consultazione pubblica finale da parte del CEN, approvato a fine marzo e pubblicato a maggio con il codice CWA 17147.

Cooperazione internazionale IECWG, GPEN, PHAEDRA *project*

Nel corso del 2017 è proseguita l'attività dei Gruppi di lavoro dedicati al coordinamento delle attività internazionali di *enforcement*, come richiesto del Gruppo di coordinamento delle attività internazionali di *enforcement* – IECWG (v. Relazione 2016, p. 165-166).

In proposito si segnala la rafforzata attività del *Global privacy enforcement network*-GPEN (la prima rete internazionale di cooperazione transfrontaliera in tema di *enforcement* di protezione dati) che nel 2017 ha dedicato il *privacy sweep* (indagine a carattere internazionale) alla verifica del rispetto della *privacy* nei siti web e applicazioni *online* in più settori – vendita al dettaglio, finanza, banche, viaggi, *social network*, giochi d'azzardo, istruzione, sanità – analizzandone le *privacy*

22

policy con l'obiettivo di verificare se per gli utenti risulti facile capire quali informazioni vengano raccolte e per quali scopi, e quali siano le modalità per il loro trattamento, utilizzo e condivisione. Il Garante, membro del GPEN, ha partecipato attivamente all'indagine sulla gestione dei dati personali in diversi settori di attività. La rete internazionale delle Autorità è giunta alle seguenti conclusioni: le informative *privacy* sono tendenzialmente generiche, prive di dettagli, e spesso formulate in modo impreciso; la maggior parte dei siti e delle *app* esaminate non informa gli utenti sull'uso che fa dei loro dati; le informative in genere non specificano a chi possono essere comunicati i dati personali raccolti; molti soggetti non spiegano agli interessati se e come i loro dati sono protetti, né come e dove sono conservati; solo in poco più della metà dei casi l'informativa spiega all'utente come esercitare il diritto di accesso ai propri dati personali. L'indagine ha evidenziato altresì che alcuni soggetti continuano a utilizzare riferimenti normativi obsoleti, e molti fra quelli che forniscono servizi a livello internazionale non sanno quale sia la normativa applicabile nei singoli Paesi. Inoltre, i siti di *e-commerce* che rilasciano fatture elettroniche spesso non forniscono alcuna informazione sulla propria attività attraverso il sito web. Anche il settore bancario, secondo l'analisi delle Autorità, non fornisce adeguate informazioni. La situazione è apparsa migliore in Italia: i siti web delle banche italiane, esaminati a campione dal Garante rispetto a quelli di altri Paesi offrono in generale agli utenti informazioni più adeguate e corrette.

Incontri con le delegazioni estere e partecipazione a progetti europei

L'Autorità ha proseguito le proprie attività nell'ambito di programmi di partenariato europeo.

A maggio si è tenuta una visita studio, della durata di tre giorni, di una delegazione dell'Autorità di protezione dei dati del Montenegro volta ad approfondire il tema della protezione dei dati nell'ambito dei settori di polizia e giustizia. L'incontro ha consentito di condividere l'esperienza ormai ventennale del Garante nell'ambito delle attività ispettive e illustrare le attività di cooperazione poste in essere con la Guardia di finanza.

Il 14 novembre il Garante ha ricevuto presso la propria sede una delegazione composta dai rappresentanti delle Banche centrali (MENA, AFRICA, ECA) e della Banca Mondiale/IFC (WBG – *World bank group*). Nell'incontro è stata illustrata l'esperienza italiana in materia di codici di condotta, in particolare nel settore delle centrali rischi e delle informazioni commerciali, sono state segnalate le novità introdotte dal RGPD e messe in luce alcune problematiche legate all'impiego dei *big data* nella cd. tecnofinanza (*Fintech*).

Il 22 novembre 2017 vi è stato un incontro tra la Commissione per la protezione delle informazioni del Giappone e il Garante. Sono state esaminate le analogie e le differenze tra la legislazione europea e giapponese in materia di protezione dei dati personali verificando le prospettive di cooperazione per una maggiore tutela della protezione dei dati personali a livello internazionale. L'Autorità giapponese in tale ambito ha illustrato l'*Act on the protection of personal information* (APPI), in vigore dal 30 maggio 2017.

Il Garante italiano e le Autorità di protezione dati di Spagna, Polonia, Croazia e Bulgaria hanno creato un consorzio, coordinato dalla Fondazione Basso, che ha vinto la selezione della Commissione europea denominata "*support training activities on the data protection reform*", volta alla formazione sull'applicazione e sull'interpretazione del RGPD.

Il progetto – che si concentra sulla formazione in relazione ai nuovi adempimenti previsti dal RGPD in ambito pubblico – si articolerà in una fase dedicata alle stesse autorità di protezione di dati al fine di affinare le loro conoscenze del RGPD e la

loro capacità di supportare le autorità pubbliche nell'adempimento della nuova normativa e si rivolgerà poi agli enti pubblici, in particolare per sensibilizzarli sulle caratteristiche e i compiti del Rpd (che, in base al RGPD, dovranno obbligatoriamente essere designati).

Il progetto (al quale partecipa anche l'Anci per l'evidente ruolo di rappresentanza e coordinamento rispetto ai comuni italiani) si fonda sulla cd. formazione dei formatori, garantendo così una trasmissione capillare delle conoscenze all'interno delle diverse strutture pubbliche chiamate ad adeguarsi ai nuovi adempimenti.

23 L'attività di comunicazione e informazione e le relazioni con il pubblico

23.1. *La comunicazione del Garante: profili generali*

L'attività di informazione e comunicazione dell'Autorità si è incentrata sulle grandi questioni legate alla dimensione digitale: dall'*hate speech* al cyberbullismo, dalla diffamazione in rete al *revenge porn*, dal diritto all'oblio alle *fake news*, dal *cybercrime* ai *big data.*

Un tema quest'ultimo che ha impegnato largamente l'Autorità in ragione del crescente impiego dei *big data* ma anche dei potenziali rischi per la riservatezza, la libertà e la dignità delle persone che il loro trattamento comporta. I *big data* sono diventati infatti un fattore strategico nella produzione, nella competizione dei mercati, nella innovazione di importanti settori pubblici e privati, ivi compresi quelli economici, nell'offerta di servizi innovativi quali quelli per la salute e per il progresso sociale.

La questione dei *big data* è stata scelta anche come tema del convegno organizzato dall'Autorità nel mese di gennaio per celebrare la Giornata europea per la protezione dei dati personali (v. *infra*).

Nel mese di giugno il Garante, insieme all'Autorità garante della concorrenza e del mercato e all'Autorità per le garanzie nelle comunicazioni, ha avviato un'indagine conoscitiva congiunta sui *big data* finalizzata anche alla definizione di un quadro di regole in grado di promuovere e tutelare la protezione dei dati personali, oltre che la concorrenza dei mercati dell'economia digitale e la tutela del consumatore (cfr. par. 14.6).

Con riguardo alla tutela della *privacy online*, va ricordata la partecipazione del Garante all'indagine internazionale (*sweep*, indagine a tappeto) condotta nel mese di maggio dalle Autorità per la protezione dei dati personali riunite nel *Global privacy enforcement network* (GPEN). I soggetti che hanno aderito all'indagine, hanno preso in esame siti e *app* in diversi settori – vendita al dettaglio, finanza e banche, sanità, istruzione, viaggi, *social network*, giochi d'azzardo – e hanno analizzato le informative sulla *privacy* con l'obiettivo di verificare il grado di trasparenza riguardo alle informazioni raccolte, agli scopi e alle modalità del loro trattamento. L'esito dell'indagine, pubblicato ad ottobre, ha evidenziato gravi carenze: in alcuni casi, le informative sono risultate incomplete non specificando, ad esempio, i soggetti a cui possono essere comunicati i dati raccolti o non spiegando se e come i dati sono protetti, né come e dove sono conservati. Spesso siti ed *app* continuano ad usare riferimenti normativi arretrati e molti dei fornitori che erogano servizi a livello internazionale mostrano di non conoscere la normativa applicabile nei singoli Paesi. In particolare le Autorità straniere hanno riscontrato nel settore bancario una generale inadeguatezza delle informazioni fornite dagli operatori mentre il Garante, sulla base dei campioni esaminati, ha verificato la disponibilità sui siti delle banche nazionali di informazioni corrette e più adeguate.

RGPD

Uno spazio centrale ha inoltre avuto la campagna di comunicazione istituzionale sul RGPD in vista della sua integrale applicazione a partire dal 25 maggio 2018. La campagna ha avuto come obiettivo principale quello di offrire indicazioni soprattutto operative per la corretta attuazione della normativa tenuto conto delle novità

introdotte a tutela dei diritti fondamentali. Sono stati in particolare studiati e realizzati, interamente *in house*, numerosi prodotti quali un opuscolo, pagine informative, infografiche, FAQ distribuiti in occasione di incontri pubblici e convegni, o diffusi mediante canali *social*, grazie ai profili istituzionali aperti dal Garante su Linkedin, YouTube e Google+.

Altri ambiti sui quali l'Autorità è intervenuta con finalità informativa sono stati il *telemarketing*, il fisco e la lotta all'evasione, la p.a. digitale, il controllo dei lavoratori, la scuola e la sanità. Anche la raccolta massiva ed indiscriminata operata dalle agenzie governative a fini di sicurezza e lotta al terrorismo, le intercettazioni e la conservazione dei dati di traffico telefonico e internet (*data retention*) hanno costituito oggetto di particolare attenzione. Nel mese di ottobre è stato firmato un nuovo protocollo d'intenti sulla protezione dei dati personali nelle attività di sicurezza cibernetica tra l'Autorità e il Dipartimento delle informazioni per la sicurezza (Dis), che conferma e rilancia le linee dell'intesa istituzionale avviata nel 2013. Il protocollo rappresenta, anche a livello europeo, un importante riferimento in materia di articolazione del rapporto tra *intelligence* e protezione dati e di bilanciamento tra il diritto alla protezione dei dati dei singoli e l'esigenza di garantire la sicurezza nazionale.

Cyberbullismo

Con riguardo al contrasto al cyberbullismo e alla violenza in rete, vieppiù diffusi, e quindi alla promozione e sensibilizzazione ad un uso responsabile e corretto dei *social network*, il Garante ha collaborato con il Miur e il *Safer internet center* – Generazioni Connesse, contribuendo all'organizzazione della prima giornata italiana contro il cyberbullismo nell'ambito del *Safer internet day* 2017. Ha inoltre svolto attività di formazione e informazione presso le classi superiori di alcuni istituti scolastici e collaborato al progetto del Comune di Roma progetto "Punti Roma Facile". Nell'ambito di questo progetto, presso le biblioteche di Roma Guglielmo Marconi e Vaccheria Nardi si sono svolte, a febbraio e a marzo, due lezioni – curate dal Servizio relazioni esterne e media – dal titolo Educazione civica digitale: guida ad un uso responsabile della rete. Durante gli incontri sono stati affrontati il tema del contrasto al cyberbullismo, della reputazione *online*, delle nuove dipendenze indotte dall'uso del web.

Ad aprile – su richiesta del dirigente scolastico del liceo scientifico Vito Volterra di Ciampino (Roma), si sono tenuti due incontri con gli studenti sul tema: *Social network* e *privacy*. Presso l'*auditorium* dell'istituto, si è svolto poi un incontro con circa 300 studenti accompagnati dagli insegnanti nell'ambito del quale sono stati trattati temi importanti come l'*hate speech*, il furto di identità, i pericoli in rete (*grooming, sextortion, revenge porn*) e le *fake news*.

Per una divulgazione delle notizie al passo con i tempi e per coinvolgere maggiormente l'utenza dei più giovani, già da qualche anno sono state rinnovate e progressivamente migliorate le strategie di comunicazione che utilizzano moderni strumenti multimediali per la realizzazione di nuovi prodotti quali: schede infografiche e pagine tematiche sempre aggiornate, video, a disposizione sul sito istituzionale e lanciati sui profilo *social* dell'Autorità, aperti su Facebook, Twitter, LinkedIn.

Tutte le questioni sopra ricordate hanno trovato interesse ed ampio riscontro sui *media*, ed in special modo sulle testate *online* ed i *blog*.

Il Servizio relazioni con i mezzi di informazione ha selezionato oltre 57.700 articoli di interesse dell'Autorità. Sulla base della rassegna stampa elaborata quotidianamente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali e dei *media online* che hanno trattato i temi legati alla *privacy* sono state 11.126 delle quali 3.102 dedicate esclusivamente all'attività del Garante. Le prime pagine sono state oltre 260 (di cui 95 riguardanti la sola Autorità). Le interviste, gli

interventi e le dichiarazioni del presidente, dei componenti del Collegio e del segretario generale, nonché dei dirigenti dei diversi Uffici e Dipartimenti dell'Autorità, sono state complessivamente 692; andate in onda su tv e radio nazionali e locali 79; le citazioni relative all'attività del Garante in programmi televisivi e radiofonici nazionali sono circa 577.

23.2. *I prodotti informativi*

Nel 2017 sono stati diffusi 41 comunicati stampa e 13 *newsletter*. Le puntate della rubrica radiofonica "*Bollettino del Garante* Privacy" sono state 18.

La *newsletter* è una pubblicazione periodica – giunta al XIX anno di diffusione (per un totale di 436 numeri e di 1.490 notizie). Nata in forma cartacea, oggi è inviata esclusivamente via *e-mail* a redazioni, professionisti, amministrazioni pubbliche, imprese e singoli che ne fanno esplicita richiesta o si iscrivono autonomamente *online* attraverso la funzione iscriviti alla *newsletter*, attiva sul sito istituzionale. Al 31 dicembre la lista di distribuzione contava 13.755 destinatari effettivi. La *newsletter* è un valido strumento di conoscenza che mette in evidenza i più importanti provvedimenti adottati dall'Autorità nei vari settori, alla sua attività in ambito sia nazionale che europeo ed internazionale, ed alle molteplici iniziative legate alla protezione dei dati personali e alla tutela dei diritti fondamentali, fornendo un vasto panorama di questioni e problematiche.

Sul sito è possibile consultare l'archivio tematico della pubblicazione che raccoglie per categorie i 19 anni di articoli prodotti dalla redazione e, sempre *online*, è consultabile anche l'intero archivio dei comunicati stampa.

Nell'attività di divulgazione va ricordata la rubrica "*Bollettino del Garante* Privacy", in onda su Radio Radicale, che illustra i principali provvedimenti adottati dal Garante e, più in generale, le tematiche legate alla protezione dei dati personali.

23.3. *I prodotti editoriali e multimediali*

La tipologia dei prodotti editoriali del Garante è ampia e differenziata e si fonda su una strategia integrata di comunicazione, nella quale spicca negli ultimi anni un crescente utilizzo della rete.

Nel 2017 soprattutto lo strumento delle schede infografiche è stato il canale comunicativo privilegiato per veicolare informazioni e concetti normativi in maniera più veloce ed intuitiva ma sempre rigorosa. Tali prodotti, che hanno da subito riscosso notevole gradimento da parte degli utenti, utilizzano un *format* compatto (una singola pagina) e sono particolarmente adatti alle esigenze di diffusione attraverso il web ed i *social media*.

I numerosi prodotti multimediali hanno offerto un ventaglio ampio di risposte alle molteplici esigenze conoscitive da parte del pubblico e semplificato la comprensione dei principali provvedimenti adottati dall'Autorità e delle nuove norme europee che interessano i diversi aspetti connessi alla protezione dei dati personali.

Per il settore editoriale meritano una menzione due nuovi volumi: "*Big data* e *privacy*. La nuova geografia dei poteri" e il "Massimario 2012-2014" pubblicati nella Collana del Garante "Contributi" nella quale sono stati raccolti nel corso degli anni testi di approfondimento sulle problematiche riguardanti la *privacy* e la tutela della dignità della persona.

Il volume "*Big data* e *privacy*. La nuova geografia dei poteri" raccoglie i contributi dei relatori intervenuti al convegno organizzato dall'Autorità in occasione della Giornata europea della protezione dei dati personali 2017(v. *infra* par. 23.4).

Riprendendo l'iniziativa avviata dal Garante negli scorsi anni, è stato pubblicato un nuovo Massimario per gli anni 2012-2014 nel corso del 2017 e per gli anni 2015-2016 nei primi mesi del 2018 (cui seguirà un terzo volume che comprenderà le massime relative agli anni 2017-2019) con l'obiettivo di facilitare l'accesso alle decisioni che hanno caratterizzato la quotidiana attività del Garante, sia sotto l'aspetto procedimentale che sostanziale.

Del testo del RGPD, il Garante ha elaborato una versione "arricchita", che segnala in corrispondenza di articoli e paragrafi i relativi "considerando" di riferimento, in modo da offrire una lettura più ampia e ragionata delle previsioni introdotte dalla nuova normativa. Il volume, realizzato in formato tascabile, è stato distribuito in occasione di incontri dedicati alle pp.aa. ed imprese. Il testo è inoltre scaricabile in formato pdf dal sito del Garante (doc. web n. 6264597).

È stata inoltre redatta la prima guida all'applicazione del RGPD che individua le principali innovazioni introdotte dalla normativa e fornisce indicazioni utili sulle prassi da seguire e gli adempimenti da attuare. Lo scopo è quello di offrire un primo strumento di ausilio ai soggetti pubblici e alle imprese e agevolare l'acquisizione di consapevolezza sulle garanzie rafforzate e sui nuovi importanti diritti che il RGPD riconosce alle persone.

Il testo è articolato in 6 sezioni tematiche: Fondamenti di liceità del trattamento; Informativa; Diritti degli interessati; Titolare, responsabile, incaricato del trattamento; Approccio basato sul rischio del trattamento e misure di *accountability* di titolari e responsabili; Trasferimenti internazionali di dati. Ogni sezione illustra in modo semplice e diretto cosa cambierà e cosa rimarrà immutato rispetto all'attuale disciplina del trattamento dei dati personali, aggiungendo preziose raccomandazioni pratiche per una corretta attuazione delle nuove disposizioni introdotte dal RGPD. La guida è disponibile sul sito del Garante (doc. web n. 6807118), anche in formato ipertestuale navigabile (doc. web n. 6302257).

Sul sito istituzionale dell'Autorità è stata predisposta una sezione appositamente dedicata al RGPD con informazioni e documenti di interesse. In particolare una pagina informativa, in continuo aggiornamento, contenente *link* alla normativa e ai documenti interpretativi; schede informative e pagine tematiche di approfondimento su argomenti specifici quali la nuova figura del responsabile della protezione dei dati (*data protection officer*), l'Autorità di controllo capofila (*lead supervisory authority)*, la valutazione d'impatto sulla protezione dei dati, i processi decisionali automatizzati e la profilazione, la notifica delle violazioni di dati personali (*data breach notification*), il diritto alla portabilità dei dati, il consenso e la trasparenza, l'applicazione e definizione delle sanzioni amministrative. Completa la già ampia campagna di comunicazione, un video istituzionale intitolato: La protezione dei dati è un diritto di libertà. Il filmato, autoprodotto dal Garante, è disponibile sia sul sito dell'Autorità che sui profili istituzionali attivati sui social media Linkedin, Google+ e Youtube e sarà trasmesso anche attraverso gli spazi televisivi offerti dalla concessionaria del servizio pubblico radiotelevisivo per la comunicazione di utilità sociale.

Nel 2017, oltre alle infografiche sopra ricordate dedicate al RGPD, sono state prodotte ulteriori schede quale quella sul cyberbullismo che sintetizza i punti principali della legge n. 71/2017 ed informa sulle nuove tutele per i minori vittime di questo preoccupante fenomeno (doc. web n. 6732832). In questo ambito l'Autorità ha predisposto anche un modulo per le segnalazioni, scaricabile dal sito

istituzionale (doc. web n. 6732688). Altra infografica è quella sui droni con la quale vengono forniti consigli per tutelare la *privacy* nel caso in cui si usi un drone a fini ricreativi (doc. web n. 6952780). È stato inoltre realizzato un video *teaser* per la promozione della campagna informativa sui droni sui *social media* (https://www.instagram.com/garanteprivacy/). Di particolare interesse la scheda sul *ransonware*, il programma informatico dannoso diffuso per infettare un dispositivo elettronico (*pc, tablet, smartphone, smart tv*), bloccandolo o criptandone i contenuti (foto, video, *file*) per poi chiedere un riscatto (*ransom*) per liberarlo. Di fronte all'aumento di questo tipo di attacchi informatici, il Garante ha predisposto una pagina informativa con alcune regole basilari per conoscere meglio questo *malware* e mettere in campo alcuni accorgimenti utili per non esserne vittima o per tentare di liberarsene nel caso in cui i dispositivi utilizzati siano già stati colpiti (doc. web n. 7307676). "E-state in *privacy*" è, invece, il titolo e di una campagna informativa sulla *privacy* nel periodo delle vacanze, comprendente un testo informativo e *badge* grafici per la comunicazione virale, contenenti informazioni utili su *selfie* e foto, protezione di *smartphone* e *tablet*, acquisti *online*, uso di *app*, *chat* e *social network* quando si è in vacanza (doc. web n. 3240343).

Infine, per celebrare i 20 anni dall'introduzione nel nostro ordinamento del diritto fondamentale alla protezione dei dati personali (8 maggio 1997), il Garante ha realizzato un video che ripercorre le tappe più significative della sua attività e i cambiamenti intervenuti nella nostra società. In questi due decenni è maturata una nuova consapevolezza sull'importanza cruciale della protezione dei dati in un mondo dove le informazioni personali sono diventate una delle nuove fonti di energia. Il Garante ha svolto un ruolo centrale nella costruzione di questa coscienza, definendo regole per il corretto uso dei dati personali, verificando l'applicazione delle norme, sanzionando le violazioni, conducendo una costante azione di sensibilizzazione, alla vigilia di uno storico cambiamento che vedrà da maggio 2018 l'applicazione in tutti i Paesi dell'Unione europea di un unico sistema di regole in materia di protezione dati. Con questo video l'Autorità ha celebrato una ricorrenza importante della storia sociale, culturale e giuridica del nostro Paese. Il video è disponibile sul sito del Garante, oltre che sui profili istituzionali attivati sui *social media* Linkedin Google+ e Youtube.

23.4. *Le manifestazioni e le conferenze*

Anche l'attività di divulgazione e approfondimento compiuta attraverso la partecipazione del presidente, dei componenti del Collegio, del segretario generale e dei dirigenti a seminari, convegni ed altre iniziative è stata come di consueto massiccia a partire da quelli sul RGPD. È stata svolta una diffusa azione di divulgazione pubblica volta ad illustrare le nuove disposizioni e chiarire le procedure operative che i soggetti coinvolti dovranno predisporre per non incorrere nella violazione delle nuove norme e nelle conseguenti sanzioni. Numerosi sono stati gli aspetti trattati: la nuova figura del responsabile della protezione dei dati personali (Rpd); la valutazione d'impatto (Dpia); il registro delle attività di trattamento; il principio di responsabilizzazione (*accountability*); il diritto alla portabilità dei dati e il diritto all'oblio; *privacy by design* e *by default* e le novità sul trattamento dei dati previdenziali e sanitari.

In questo ambito, si segnala anche il convegno organizzato dal Garante per celebrare l'XI edizione della Giornata europea della protezione dati dal titolo *"Big data* e *privacy*. La nuova geografia dei poteri" (30 gennaio – Aula del Palazzo dei Gruppi

parlamentari) (doc. web n. 5892736), preziosa occasione di riflessione sull'impatto dei *big data* sull'organizzazione sociale e i processi decisionali anche sotto il profilo delle prospettive che essi aprono all'intelligenza artificiale e alla genomica, sul nuovo capitalismo digitale e sui i nuovi modelli di *business*.

Nella prima sessione "La nuova economia fondata sui dati" – coordinata da Augusta Iannini, vicepresidente dell'Autorità – sono intervenuti Franco Bernabè e Giulio Tremonti. Nella seconda sessione "Dal profilo dei consumatori al profilo dei cittadini", coordinata da Licia Califano, sono intervenuti Ilvo Diamanti ed Enrico Giovannini. Nella terza sessione, dedicata a "Le grandi sfide: *open data*, genomica, intelligenza artificiale", gli interventi di Diego Piacentini e Stefano Ceri sono stati coordinati da Giovanna Bianchi Clerici. I lavori sono stati aperti dal presidente Soro che ha focalizzato l'attenzione sulle dinamiche con le quali lo sviluppo tecnologico è destinato a mutare i rapporti di potere nella società globale, cambiando i modelli e le abitudini della politica e dell'esercizio dei diritti come la riservatezza e la protezione dei dati personali. Il presidente Soro nel suo intervento ha richiamato l'attenzione sulle criticità connesse all'uso dei *big data* e in particolare sul rischio di consegnare a poche multinazionali digitali non soltanto la supremazia economica, ma anche il potere di conoscere i fenomeni idonei a governare e influenzare il nostro sapere. Ha concluso i lavori il Ministro per i rapporti con il Parlamento, on. Anna Finocchiaro.

In occasione della Giornata europea, come ogni anno, sono stati invitati a partecipare al convegno, tra gli altri, gli studenti di due licei romani allo scopo di coinvolgere le giovani generazioni su temi di grande impatto e valore sociale, economico e culturale come quelli legati alla protezione dei dati personali.

Il 27 novembre, per l'XI anno consecutivo, *Consumers' Forum*, associazione indipendente composta dalle più importanti associazioni di consumatori, istituzioni, numerose imprese industriali e di servizi e loro associazioni di categoria, ha organizzato un incontro con le maggiori Authority italiane per presentare la ricerca "Consumerism2017", dal titolo "Dalla *sharing* alla *social economy*, alla data *economy, big data*, *fake news*, *privacy* e pubblicità" e riflettere insieme sulle nuove sfide dei mercati e le forme di tutela dei consumatori.

Il presidente Soro ha ricordato come sia necessario "evitare, da una parte, di attribuire ai gestori delle piattaforme digitali il ruolo di semaforo, lasciando loro una discrezionalità totale nella individuazione di contenuti lesivi e, dall'altra, di immaginare di attribuire ad un algoritmo il compito di arbitro della verità". Una posizione, questa, che si porrebbe, ad avviso del presidente, "in controtendenza non solo rispetto alla storia del diritto, ma anche della cultura democratica".

Il 14 settembre, il presidente Soro ha partecipato al convegno internazionale "Sicurezza e linguaggio dell'odio. Tutela della persona e protezione dei dati personali: i diritti nell'era dei *social media*", promosso dal Consiglio nazionale forense in occasione della presidenza italiana del G7.

Di fronte all'aumentare delle diseguaglianze sociali e alla difficoltà dell'ordinamento di porsi al passo con l'innovazione, la protezione dei dati si è rivelata, secondo il presidente Soro, risorsa indispensabile per garantire un corretto equilibrio tra mercato e individuo, informazione e dignità, tecnica e vita. "Le grandi imprese del web hanno acquisito poteri la cui rilevanza non si esaurisce sul piano economico e commerciale, ma entra in una dimensione sociale, politica. I gestori delle piattaforme sono chiamati, ad esempio, dalla legge sul cyberbullismo, a rimuovere contenuti illeciti. Se la loro responsabilizzazione concorre dunque a ridurre l'uso violento della rete, spetta tuttavia allo Stato impedire che internet diventi terreno in cui si può violare la dignità delle persone".

23

L'Autorità ha partecipato anche all'iniziativa lanciata da Google per promuovere tra i più giovani l'uso consapevole e sicuro delle risorse offerte dal web. La campagna, denominata "Digitali e responsabili. Il cittadino digitale, quali responsabilità?" ha offerto, attraverso una serie di tappe in alcune delle principali università italiane, spunti di riflessione e confronto su temi diversi legati al settore *online*. Il progetto è stato presentato a Roma il 6 luglio ed in tale occasione il presidente Soro ha sottolineato quanto sia importante "nello scenario digitale essere cittadini responsabili e orgogliosi difensori dei propri diritti. Della protezione dei dati in primo luogo, che è il nuovo nome della libertà".

In ricordo del professor Stefano Rodotà, scomparso il 23 giugno 2017, il presidente Soro ha preso parte all'incontro organizzato presso la Fondazione Basso il 6 ottobre ricordandone lo straordinario contributo alla Fondazione e allo sviluppo della cultura del diritto alla protezione dei dati personali nel nostro Paese.

23.5. *L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi*

Il 2017 ha visto l'Ufficio relazioni con il pubblico – primo e diretto interlocutore del Garante verso l'esterno – intensamente impegnato nello svolgimento delle diverse attività cui è preposto e che consistono principalmente nella consulenza ai visitatori in sede e nell'assistenza telefonica nonché nella gestione delle richieste pervenute via *e-mail* (con la definizione di 300 affari e 200 visitatori ricevuti presso la sede dell'Ufficio: cfr. sez. IV, tab. 15 e 16). L'attività svolta – che consente all'Urp di cogliere in tempo reale le problematiche di maggiore rilevanza sociale o economica, da sottoporre all'attenzione dell'Autorità (anche mediante *report* interni) – si è concentrata in modo particolare sulle richieste di chiarimenti riguardanti il RGPD, oltre che sui quesiti relativi alle modifiche introdotte in ambito sanitario dal decreto legge 7 giugno 2017, n. 73, recante disposizioni urgenti in materia di prevenzione vaccinale, di malattie infettive e di controversie relative alla somministrazione di farmaci, convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 31 luglio 2017, n. 119 (v. par. 5.2.1).

Al fine di migliorare l'offerta informativa e consentire ad un maggior numero di interessati di ricevere le informazioni e i chiarimenti desiderati, l'Urp ha poi curato la predisposizione di schede informative in materia di *telemarketing*, videosorveglianza e esercizio dei diritti. Tali schede sono state utilizzate anche nell'ambito delle procedure introdotte a seguito dell'istituzione di un risponditore automatico, allo scopo di fornire prime informazioni all'utenza su specifici argomenti. Ciò ha consentito di assicurare una prima assistenza telefonica anche a chi si rivolge all'Urp nelle ore di chiusura o quando, a causa dell'ingente numero di chiamate gestite giornalmente, le linee risultano occupate.

I contatti gestiti sono stati anche quest'anno numerosi: circa 16.200 richieste, delle quali 10.900 circa pervenute via *e-mail*. Numeri che attestano il persistente alto livello di attenzione dell'opinione pubblica nei confronti della protezione dei dati personali e dell'attività svolta dal Garante.

Tematiche d'interesse

Tra le molteplici questioni concernenti la normativa in materia di protezione dei dati personali sottoposte all'Urp nel 2017, si segnalano in particolare quelle di seguito riportate, oggetto di maggiore attenzione da parte dell'opinione pubblica o del dibattito istituzionale.

Nonostante una flessione del numero delle segnalazioni rispetto all'anno precedente, dovuta principalmente ai nuovi strumenti informativi messi a disposizione dell'utenza (FAQ e informazioni fornite dal risponditore automatico), al primo

posto c'è ancora il *telemarketing* che continua ad essere fonte di grande disturbo, come confermano le circa 2.000 *e-mail* ricevute, parte delle quali riguarda il fenomeno delle cd. chiamate mute. Grande interesse hanno suscitato le nuove previsioni contenute nella legge 11 gennaio 2018, n. 5 recante nuove disposizioni in materia di iscrizione e funzionamento del Registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato. Ha in particolare destato interesse l'introduzione della facoltà di iscrizione nel Rpo dei numeri di telefono mobile e di tutti i numeri cd. riservati, vale a dire delle utenze non presenti negli elenchi telefonici pubblici.

Anche il *marketing* via sms, fax e *e-mail* continua ad essere al centro dell'attenzione, come confermano le oltre 800 segnalazioni ricevute. Si ricordano inoltre, sempre con riguardo ai trattamenti svolti in ambito TLC, le questioni relative alle attivazioni di servizi a pagamento non richiesti sulle utenze di telefonia mobile effettuate nel corso della navigazione in internet nonché le richieste degli utenti relative all'accesso ai dati di traffico telefonico e telematico, sia in uscita sia in entrata.

Il maggior numero di richieste di chiarimento ha riguardato la nuova normativa introdotta dal RGPD ed in particolare i nuovi principi, *in primis* quello di responsabilità del titolare del trattamento, la designazione del responsabile della protezione dei dati personali, la valutazione di impatto e la tenuta dei registri delle attività di trattamento. Altrettante istanze, pervenute soprattutto da imprese e pp.aa, hanno avuto ad oggetto il rapporto tra le disposizioni del RGPD e gli articoli del Codice relativi ad ambiti non direttamente interessati dalla modifica normativa, rispetto ai quali si attende l'adozione dei decreti previsti dalla legge 25 ottobre 2017, n. 163, che ha delegato il Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea (legge di delegazione europea 2016-2017).

Particolare interesse hanno suscitato, come già anticipato, le modifiche introdotte in ambito sanitario e scolastico dal decreto legge 7 giugno 2017, n. 73, recante disposizioni urgenti in materia di prevenzione vaccinale, di malattie infettive e di controversie relative alla somministrazione di farmaci, convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 31 luglio 2017, n. 119. Al riguardo, l'Ufficio ha fornito chiarimenti a seguito dell'adozione da parte del Garante di un provvedimento urgente che autorizza una comunicazione di dati personali non sensibili dalle scuole alle autorità sanitarie, previsto dalla legge solo dall'anno scolastico 2018-2019 (provv. 1° settembre 2017, n. 365, doc. web n. 6765917).

Sempre al centro di numerose istanze, pervenute sia da enti pubblici sia da singoli, è stato il tema concernente i trattamenti di dati personali effettuati da soggetti pubblici per finalità di pubblicità e trasparenza sul web.

Anche nel 2017 numerosi quesiti e richieste hanno riguardato la videosorveglianza, con particolare riguardo all'ambito condominiale e scolastico. In tale ultimo contesto, l'Ufficio ha fornito spesso chiarimenti in merito alla possibilità per gli studenti di registrare le lezioni a fini di apprendimento.

Grande interesse hanno poi suscitato le questioni concernenti i trattamenti di dati personali nell'ambito della rete internet e dei *social network*, con richieste di assistenza provenienti, soprattutto a seguito dell'entrata in vigore della legge 29 maggio 2017, n. 71 (Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo), anche da soggetti minori di età, ai quali l'Urp ha risposto sempre in tempi brevissimi. Molte istanze hanno riguardato anche i trattamenti in ambito giornalistico e, in particolare, la gestione dei cd. archivi storici *online* dei quotidiani.

23

Anche il contesto lavorativo permane al centro di numerose richieste relative all'utilizzo delle telecamere, 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 mediante l'uso di sistemi di rilevazione biometrica.

Numerose sono state anche le richieste relative agli adempimenti e agli strumenti di tutela previsti dal Codice (oltre 1.500 *e-mail*) e ciò conferma la consapevolezza e l'attenzione degli utenti in merito alle garanzie riconosciute dal Codice.

Si segnalano, infine, le questioni concernenti i trattamenti di dati nell'ambito dei sistemi di informazioni creditizie e l'accesso ai dati bancari, nonché le richieste relative al codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale.

24 Studi, documentazione e biblioteca

24.1. *Il Servizio studi e documentazione*

Relazione annuale

Il Servizio studi e documentazione ha coordinato la predisposizione del testo della Relazione annuale sull'attività svolta nel 2016 e sullo stato di attuazione del Codice, che rappresenta un fondamentale adempimento istituzionale dell'Autorità previsto dall'art. 154, comma 1, lett. *m*), del Codice, il quale individua tra i compiti del Garante anche la rappresentazione dell'attività svolta nell'anno solare di riferimento per la presentazione al Parlamento e al Governo. Il Servizio ha anche avviato l'attività preparatoria per la redazione della Relazione riferita all'anno 2017.

Il Garante ha dato attuazione alla previsione, introdotta nel 2014, secondo cui le autorità amministrative indipendenti sono tenute a dare conto nella Relazione annuale del rispetto delle disposizioni concernenti la razionalizzazione delle spese e sono tenute alla trasmissione della Relazione anche alla Corte dei conti (art. 22, d.l. n. 90/2014 convertito in l. 11 agosto 2014, n. 114).

La pubblicazione sul sito istituzionale del Garante della Relazione annuale consente di perseguire una finalità di trasparenza sull'attività svolta dall'Autorità non soltanto rispetto ai soggetti destinatari *ex lege* della Relazione ovvero il Parlamento, il Governo e la Corte dei conti, ma anche nei confronti della collettività e, al contempo, rappresenta un prezioso strumento di conoscenza per diverse categorie di utenti interessati, a vario titolo, all'applicazione della disciplina riguardante la protezione dei dati personali. In questa prospettiva, la struttura della Relazione, che presenta tradizionalmente sia una parte generale ed introduttiva sui più significativi interventi effettuati dall'Autorità nel periodo di riferimento sia molteplici sezioni tematiche (ivi comprese quelle di natura statistica), consente di fornire, in modo rapido e sintetico, informazioni puntuali sull'attività svolta (con particolare riguardo all'attività provvedimentale, sanzionatoria e comunicativa, nonché a quella svolta in ambito europeo ed internazionale) ed aggiornamenti su specifici profili o istituti attinenti alla protezione dati.

Attività di studio, documentazione e supporto giuridico

Studi e ricerche sono state condotte su questioni tecnico-giuridiche di attualità – si pensi al supporto interno fornito circa l'interpretazione e l'attuazione delle innovazioni in materia di prevenzione della corruzione e di trasparenza (modifiche apportate dal decreto legislativo n. 97/2016 alla legge n. 190/2012 e al decreto legislativo n. 33/2013) – o comunque di interesse dell'Autorità, anche in forma di *dossier* (ad es., con un'ampia analisi comparativa, rispetto a modelli normativi e organizzativi stranieri in materia di *data protection*, finalizzata anche a supportare gli interventi di riorganizzazione del Garante funzionali alla piena attuazione del RGPD).

L'attività di documentazione viene svolta mediante il costante monitoraggio della giurisprudenza, dottrina e documentazione nazionale, comunitaria ed internazionale, in particolare in materia di protezione dati, con la predisposizione di un osservatorio ad uso interno. Al riguardo, a titolo meramente esemplificativo, si menzionano tra le questioni segnalate quelle in tema di parto anonimo e ricerca delle proprie origine da parte dell'adottato (Corte di cassazione n. 1946/2017), diffamazione attraverso internet e responsabilità del *provider* (Corte di cassazione nn. 2723, 4873/2017 e 54946/2016), *ne bis in idem* (Corte di cassazione nn. 9184,

41528/2017; CEDU caso Sinkus c/Lituania 13 giugno 2017; conclusioni dell'Avvocato generale presentate il 12 settembre 2017 nelle cause C-524/15, C-537/16 e nelle cause riunite C-596/16 e C-597/16), accesso abusivo a sistema informatico (Corte di cassazione, S.U. nn. 41210/2017 e 48370/2017).

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 è costituito da ca. 29.000 documenti bibliografici, con ca.15.000 monografie, opuscoli ed estratti di pubblicazioni, 7.500 dei quali in lingua straniera, ed 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. Complessivamente, il patrimonio bibliografico della Biblioteca si estende su ca. 480 metri lineari di scaffalature. 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 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 e di predisposizione delle operazioni di trasloco nella nuova sede, l'Ufficio ha temporaneamente trasferito l'intero patrimonio della biblioteca in magazzini, in vista del riallestimento di una o più sale di lettura e di consultazione. Allo stesso tempo sono stati avviati contatti con importanti istituzioni bibliotecarie per una collaborazione utile al completamento della catalogazione del posseduto in Opac e la sua immissione in internet.

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 specializzata multilingue 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, tramite interventi sul mercato librario internazionale dell'usato, assume un particolare rilievo nel panorama delle biblioteche giuridiche. Per quanto concerne una valutazione comparata del patrimonio bibliografico della biblioteca dell'Autorità, valgano i seguenti riscontri statistici (aggiornati al 31 dicembre 2017): il sistema SBN cataloga con il vocabolo "*privacy*" nel titolo 1.410 documenti (1.243 monografie, +67 sul 2016, 735 delle quali in italiano); 224 documenti (195 monografie) con la stringa *"protezione dei dati"* nel titolo; 204 documenti (189 monografie) con la stringa *"data protection"*; 78 documenti (78 monografie) con la stringa "*Datenschutz*".

I cataloghi del Polo bibliotecario parlamentare registrano sotto la voce "riservatezza" 1137 documenti e sotto la voce "*privacy*" 550. I *records* aventi il vocabolo "*privacy*" nel titolo sono 373 (+15 sul 2016, 218 dei quali in italiano, 125 alla

Camera e 93 al Senato); quelli aventi nel titolo la stringa "*protezione dei dati*" sono 140 (+11 sul 2016); quelli con l'espressione *"data protection*" 70 (+11 sul 2016); quelli con il vocabolo "*Datenschutz"* 50 (+4 sul 2016). In Germania, la *Deutsche Nationalbibliothek* conta 1.579 documenti con il vocabolo "*privacy*" nel titolo (529 monografie, 1.037 risorse *online* e 473 articoli) e 146 monografie con il vocabolo "*Datenschutz*" pubblicate dopo il 2016. Negli Stati Uniti, la principale biblioteca giuridica mondiale, la Harvard Law School Library, cataloga sotto la voce onnicomprensiva "*privacy*" ben 2.401.240 documenti (1.805.852 dei quali disponibili *online*), così ripartiti: 88.681 pubblicazioni monografiche (1.244 pubblicate dopo il 2016); 287 monografie in lingua italiana; 901.797 articoli di quotidiani; 863.906 articoli scientifici e di spoglio.

Nel 2017 i servizi all'utenza interna ed esterna hanno funzionato in modo ridotto a causa del nuovo trasloco e dei trasferimenti delle collezioni nei magazzini. Questi i dati relativi agli utenti interni: 22 i documenti richiesti in lettura; 14 i prestiti; 62 i casi di assistenza bibliotecaria (60 *online*); 26 le riproduzioni di documenti con inoltro in formato elettronico. Questi i dati sul pubblico esterno: 7 le autorizzazioni alla frequentazione; 24 i casi di assistenza bibliografica *online*; 8 gli invii di *document delivery*. La consultazione del catalogo Opac sulla intranet ha registrato 2.005 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. La scelta dell'Ufficio, davanti alla situazione di oggettiva emergenza prodotta dal susseguirsi delle operazioni di trasloco delle collezioni della biblioteca, è stata quella di potenziare il progetto di *digital library* e di valorizzare i *database* giuridici consultabili sul sito intranet della biblioteca attraverso specifici corsi di formazione. Gli elaborati statistici indicano che il numero totale dei documenti consultati nel 2017 ha confermato il superamento del traguardo delle 150.000 operazioni (cifra ottenuta sommando il numero di ricerche e quello delle visualizzazioni), con un incremento di ca. il 10% rispetto al 2016, anno che aveva già fatto registrare il *record* di oltre 150.000 operazioni. Il *database* con il più elevato conteggio ha registrato 7.892 sessioni di lavoro (7.516 nel 2016, 6.864 nel 2015, 6.814 nel 2014, 6.529 nel 2013, 5.828 nel 2012, 4.889 nel 2011 e 4.052 nel 2010) e 93.556 documenti consultati (89.103 nel 2016, 75.147 nel 2015, 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. 36 connessioni e 425 documenti (34 connessioni e 405 documenti nel 2016, 30 connessioni e 326 documenti nel 2015, 30 connessioni e 364 documenti nel 2014, 28 connessioni e 337 documenti nel 2013).

L'Ufficio del Garante

III - L'Ufficio del Garante

25 La gestione amministrativa e dei sistemi informatici

25.1. *Il bilancio e la gestione economico-finanziaria*

L'assetto amministrativo-contabile dell'Autorità è improntato ai princìpi generali della contabilità finanziaria, economica e patrimoniale, nel pieno rispetto delle procedure e dei termini prescritti dalle disposizioni di legge e regolamentari volti ad assicurare una generale esigenza di armonizzazione dei sistemi contabili pubblici.

Nel corso dell'intero esercizio la gestione si è svolta in base al bilancio di previsione, approvato entro i prescritti termini regolamentari, avendo cura di contemperare il perseguimento delle finalità istituzionali e degli obiettivi definiti nell'ambito del documento programmatico con le risorse finanziarie disponibili.

Diversamente da quanto previsto per i precedenti esercizi finanziari nei quali il finanziamento del Garante prevedeva, in aggiunta alle risorse di provenienza erariale, un contributo da parte di altre Autorità indipendenti, la gestione del 2017 è stata caratterizzata da una maggiore stabilità delle entrate per effetto delle misure contenute nella legge europea 2015-2016 (l. 7 luglio 2016, n. 122) che ha posto a carico del bilancio dello Stato l'integrale onere di funzionamento dell'Autorità. Tale modifica ha consentito una migliore programmazione delle attività nella prospettiva della definitiva entrata in vigore del regolamento UE in materia di trattamento dei dati personali. Nella medesima prospettiva, si è preso atto favorevolmente delle ulteriori misure che il legislatore, al fine di porre l'Autorità nella migliore condizione per assolvere i compiti in materia di protezione dei dati assegnati dal legislatore nazionale e quelli derivanti dagli obblighi di appartenenza all'Unione europea, ha adottato nel corso dell'anno a vantaggio del Garante, sia con la legge europea 2017 (art. 29, l. 20 novembre 2017, n. 167), sia con la legge di bilancio (l. 27 dicembre 2017, n. 205), i cui effetti finanziari decorrono in massima parte dall'anno 2018.

All'interno di un quadro finanziario di riferimento sostanzialmente migliorato, va segnalato che il bilancio è stato comunque improntato ad una prudente valutazione delle entrate e ad una attenta programmazione delle spese, anche in considerazione di taluni perduranti vincoli di spesa definiti nell'ambito di atti e provvedimenti legislativi.

Tra le diverse misure adottate negli anni, confermate anche nel corso dell'esercizio finanziario 2017, si segnala che nell'intero periodo di riferimento non sono stati conferiti incarichi di consulenza.

Appare inoltre doveroso precisare che il Garante, per fare fronte alle esigenze di mobilità istituzionale e di servizio, fruisce di un'unica autovettura assegnata in comodato gratuito dalla competente autorità governativa, le cui spese si limitano ai soli oneri di gestione. L'Autorità non detiene immobili adibiti ad abitazione o foresteria.

25

Con riferimento alla generalità della spesa strettamente connessa alle esigenze gestionali, si evidenzia che nel corso dell'anno risultano rispettati, tra l'altro, i limiti riguardanti la spesa complessiva per consumi intermedi (art. 8, comma 3, d.l. 6 luglio 2012, n. 95, convertito, con modificazioni, dalla l. 7 agosto 2012, n. 135 e successive integrazioni).

Si segnala, da ultimo, che le indennità di carica dei componenti del Garante non hanno subito variazioni ed il loro importo resta contenuto entro i prescritti limiti di legge.

L'intera gestione è stata oggetto di periodici controlli da parte del preposto organo interno di revisione amministrativo-contabile di cui fa parte, per espressa decisione della stessa Autorità, un magistrato contabile e due alti dirigenti pubblici esperti in materia: la composizione dell'organo e la professionalità dei relativi componenti intende costituire ulteriore garanzia di corretta attività gestionale.

Inoltre, in conformità alle vigenti disposizioni sugli obblighi di trasparenza, le principali evidenze contabili, a partire dai bilanci di previsione e consuntivi, sono periodicamente resi pubblici nell'ambito della specifica sezione del sito web istituzionale.

Quanto ai risultati registrati nel corso dell'esercizio, si evidenzia che la gestione di cassa ha prodotto incassi per complessivi 25,6 milioni di euro e pagamenti totali per 24,8 milioni di euro; tali valori hanno generato un incremento delle disponibilità finali di periodo del saldo di cassa di 0,8 milioni di euro.

La gestione economico-finanziaria ha determinato un risultato positivo di 1,6 milioni di euro, scaturito dalla differenza tra le entrate e le uscite di competenza. Tale valore risulta in linea con una generale tendenza di sostanziale equilibrio finanziario costantemente registrato dall'Autorità negli anni, a conferma di una gestione attenta ed equilibrata.

In estrema sintesi, si precisa che le entrate di competenza dell'esercizio complessivamente registrate in bilancio sono state 21,0 milioni di euro a fronte delle quali sono stati assunti impegni di spesa per 19,4 milioni di euro.

A differenza del precedente esercizio, nel quale i trasferimenti erariali rappresentavano un valore inferiore al 50% delle entrate complessive dell'Autorità, le modifiche delle fonti di finanziamento previste a decorrere dal 2017 dalla richiamata l. n. 122/2016 hanno ricondotto il fabbisogno occorrente per il funzionamento del Garante in via pressoché esclusiva nell'ambito delle risorse stanziate a carico del bilancio dello Stato (per il 2017 oltre il 96% del totale) mentre soltanto una parte residuale delle entrate acquisite al bilancio attengono a risorse proprie dell'Autorità derivanti da diritti di segreteria e rimborsi di varia natura.

La tabella 19 (cfr. sez. IV) evidenzia i risultati sintetici della gestione relativa al 2017 posti in relazione agli analoghi valori del precedente esercizio. Dal raffronto emerge la modifica della struttura di finanziamento dell'Autorità che nel complesso determina un incremento di entrate nella misura del 5,9%.

Per quanto riguarda le uscite, invece, si registrano nell'esercizio di competenza valori che in termini assoluti si discostano poco rispetto a quelli del precedente anno, a conferma di un tendenziale di spesa nel complesso sostanzialmente stabile.

In particolare, le uscite di natura corrente, nell'ambito delle quali sono comprese le spese di funzionamento e quelle per il personale, fanno registrare un incremento di circa l'1,1% ascrivibile in massima parte alla naturale dinamica di crescita degli oneri per il personale.

La spesa è caratterizzata da una struttura che ricalca la composizione che caratterizza la generalità dei soggetti pubblici dove l'incidenza degli oneri per il personale assume un peso significativo. Nel caso specifico del Garante, poi, le risorse umane

rappresentano una componente ineludibile in ragione dell'elevato livello di professionalità ed esperienza che il settore specifico richiede per le delicate funzioni da svolgere anche attraverso una sempre maggiore partecipazione nelle pertinenti sedi istituzionali europee.

In termini complessivi, il più significativo incremento delle entrate rispetto ad una più contenuta crescita della spesa determina, come risultato della gestione corrente, un valore positivo, con un avanzo di amministrazione pari alla misura sopra indicata di 1,6 milioni di euro.

25.2. *L'attività contrattuale, la logistica e la manutenzione degli immobili*

Attività contrattuale

Nell'anno 2017 l'attività dell'Autorità concernente i contratti pubblici è proseguita in linea con l'attuazione degli obiettivi del Garante e in conformità alla normativa vigente, la quale in particolare prevede che le Autorità amministrative indipendenti, al fine di dare attuazione alle esigenze di razionalizzazione, sono tenute a gestire "i servizi strumentali in modo unitario, mediante la stipula di convenzioni o la costituzione di uffici comuni ad almeno due organismi" (cfr. art. 22, d.l. 24 giugno 2014, n. 90 convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 11 agosto 2014, n. 114).

Per quanto precede, ampie interlocuzioni con l'Autorità per l'energia, il gas ed il servizio idrico (ora Arera), nonché con l'Autorità di regolazione dei trasporti, hanno consentito l'individuazione di un percorso comune per la gara relativa al programma di assistenza sanitaria e malattia dei componenti del Collegio e del personale delle Autorità; tale gara, di rilevanza comunitaria e a procedura ristretta, è stata bandita nel mese di luglio 2017 e si è conclusa nel mese di marzo 2018. Nel corso dell'anno è stata altresì avviata una seconda procedura di gara comunitaria, in comune questa volta con l'Autorità per le garanzie nelle comunicazioni e con l'Autorità di regolazione dei trasporti, relativa ad ulteriori servizi assicurativi quali la sede, il patrimonio mobiliare, la responsabilità civile; la procedura è stata indetta nel mese di ottobre 2017, con atti pubblicati nel mese di gennaio 2018, a seguito delle necessarie interlocuzioni con le citate Autorità. I lotti di interesse di questa Autorità sono quattro, con inizio dei servizi previsto a giugno 2018. Sempre riguardo alle gare di rilevanza europea, è stata espletata una procedura aperta, relativa al servizio di protocollazione e assistenza in materia di amministrazione digitale.

Durante il periodo in considerazione sono stati ampiamente utilizzati, come già in passato, gli strumenti messi a disposizione da Consip s.p.a. sul portale Acquistinretepa.it; oltre alle convenzioni, è stato utilizzato lo strumento dell'accordo quadro e sono stati realizzati numerosi acquisti a mezzo Richiesta di offerta (Rdo), Trattativa diretta (Td) ed Ordine diretto d'acquisto (Oda) sul Mercato elettronico della p.a. (Mepa), nei termini previsti dalla normativa.

In particolare, l'Ufficio ha utilizzato l'accordo quadro Consip denominato "Centrali telefoniche ed. n. 7" per sostituire le proprie apparecchiature di centralino, ormai obsolete e non in grado di assicurare la dovuta connessione tra le due sedi di piazza di Monte Citorio e di piazza Colonna in cui sono, allo stato, situati gli uffici dell'Autorità. Relativamente alle convenzioni Consip, invece, l'Autorità ha aderito a quelle relative all'acquisto di stampanti *desktop* (stampanti 14) e al noleggio di fotocopiatrici multifunzione (ed. n. 26). Le Rdo sul Mepa, qualora di importo superiore a 40.000 euro, sono state sempre precedute – in applicazione delle linee guida dell'Anac – da pubblicazione di avvisi di gara sul sito internet dell'Autorità, per almeno 15 giorni. Riguardo all'oggetto, le Rdo hanno riguardato,

25

per circa il 90% dell'importo affidato, forniture di *hardware*, di *software* e di servizi connessi, tra le quali preponderante, dal punto di vista dell'importo, è stata quella relativa alla sostituzione del sistema di protocollazione ed amministrazione digitale. Il ribasso medio realizzato nell'effettuazione delle predette procedure è stato pari a circa il 19%. Sempre sul Mepa sono state effettuate Td ed Oda, per importi medi di circa 5.500,00 euro, che hanno riguardato un ampio ventaglio di categorie merceologiche.

Con riferimento alle previsioni di cui alla legge di stabilità 2016 (art. 1, comma 512, l. 28 dicembre 2015, n. 208), si evidenzia che tutti gli acquisti di *hardware* e *software* sono stati effettuati utilizzando i summenzionati strumenti di acquisto e negoziazione del portale Consip, salvo una fornitura di limitato importo (euro 3.750), non disponibile sul predetto portale e connessa a licenze acquisite in precedenza.

Come sarà meglio chiarito a seguire, è proseguita nel 2017 l'attività finalizzata alla individuazione di una nuova sede dell'Ufficio, attività ancora in corso di definizione. Ciò ha comportato, tra l'altro, riflessi in merito a taluni servizi connessi alla sede (*facility management*, vigilanza), riguardo ai quali la situazione di sostanziale incertezza non ha consentito l'avvio di procedure di gara.

Sono state effettuate alcune proroghe contrattuali, in costanza dei relativi presupposti, per la necessità di continuare l'erogazione dei servizi durante il tempo di svolgimento delle apposite gare d'appalto (ad esempio servizi di protocollazione, assistenza sanitaria per il personale del Garante, altre coperture assicurative sopra menzionate) nonché per la mancata attivazione di nuove convenzioni da parte di Consip, nei tempi previsti; tale ultima fattispecie ha riguardato, in particolare, il richiamato contratto di *facility management* per la sede dell'Autorità, prorogato fino al 31 dicembre 2018 salvo attivazione della nuova convenzione Consip *facility management* 4, in relazione alla quale, secondo quanto comunicato da Consip, il termine del relativo procedimento di gara è previsto entro il 29 giugno 2018.

Come già nel 2016, un significativo impegno di risorse è stato destinato alla gestione della delicata fase di prima attuazione del d.lgs. n. 50/2016 (nuovo codice dei contratti pubblici), anche alla luce delle significative integrazioni apportate dal decreto correttivo (d.lgs. n. 56/2017) e dalle conseguenti linee guida Anac, tuttora in corso di aggiornamento; sono state apportate alcune modifiche alla regolamentazione interna dell'Autorità e sono state altresì avviate, con gli uffici dell'Autorità, le attività finalizzate alla definizione della programmazione biennale degli acquisti, in attuazione del nuovo codice, alla cui pubblicazione si è provveduto secondo la tempistica prevista.

È infine proseguita l'attività di attuazione delle disposizioni in materia di trasparenza, alla luce delle significative innovazioni normative del settore; a tal fine l'Ufficio ha avviato, a fine 2017, una gestione integrata della procedura di predisposizione delle gare di appalto, mediante apposito *software*.

Logistica e manutenzione degli immobili

Impegnativa è risultata l'attività volta all'individuazione della nuova sede dell'Autorità. Le importanti sopravvenienze verificatesi nel periodo in questione, sia sotto il profilo normativo (ampliamento del ruolo organico dell'Ufficio per n. 25 unità, in connessione con la prossima entrata in vigore del RGPD), sia dal punto di vista fattuale, per la riduzione degli spazi effettivamente utilizzabili nell'ambito della sede oggetto di contratto di locazione stipulato a fine 2016 con la società di gestione immobiliare Igei s.p.a. in liquidazione – Inps, hanno reso necessario recedere dal contratto con quest'ultima e indire un'ulteriore procedura di ricerca di mercato. Tale procedura, tuttora in corso e svolta con l'assistenza

dell'Agenzia del demanio, si è rivelata particolarmente complessa. Allo stato, pertanto, l'Ufficio resta suddiviso, come detto, nelle due sedi limitrofe di Piazza di Monte Citorio e Piazza Colonna, nelle more della individuazione di una sede unica, idonea alle rinnovate esigenze dell'Autorità e a semplificate attività di manutenzione ordinaria e logistica.

25.3. *L'organizzazione dell'Ufficio: il personale ed i collaboratori esterni*

In conformità alle disposizioni previste dal d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122, nel periodo considerato non sono stati conferiti incarichi di consulenza.

Con riguardo alla convenzione quadro in materia di procedure concorsuali congiunte per il reclutamento del personale delle Autorità indipendenti, siglata nel 2015 ai sensi dell'art. 22, comma 4, d.l. n. 90/2014, sono state bandite da altre Autorità indipendenti alcune procedure concorsuali alle quali tuttavia il Garante, in ragione della specificità dei profili richiesti, non ha ritenuto di aderire, attivando due procedure di mobilità volontaria esterna per funzionari, espletate nel corso dello stesso anno.

A seguito delle due menzionate procedure di mobilità volontaria esterna, indette ai sensi dell'art. 30, d.lgs. n. 165/2001, sono stati immessi in ruolo cinque funzionari, di cui tre con profilo informatico/tecnologico e due con profilo giuridico/amministrativo. Nel corso dell'anno, è stata altresì distaccata in comando una funzionaria presso la Presidenza del Consiglio dei ministri; un funzionario è stato collocato in quiescenza. Nell'anno considerato si è quindi verificato un complessivo incremento di tre unità di personale in servizio.

Si è inoltre provveduto a svolgere due procedure per la selezione di 10 giovani laureati per l'effettuazione di periodi di tirocinio presso l'Autorità.

Al 31 dicembre 2017 l'Ufficio poteva così contare su un organico, a diverso titolo, di 137 unità, di cui 116 in servizio, al quale andava aggiunto un contingente di personale a contratto di otto unità, tutte in servizio (cfr. sez. IV, tab. 17 e 18).

Inoltre, come anticipato, con l. 20 novembre 2017, n. 167 è stato introdotto un incremento del ruolo organico del Garante in misura pari a 25 unità anche allo scopo di meglio assicurare il regolare esercizio dei poteri di controllo affidati al Garante per la protezione dei dati personali e per fare fronte agli accresciuti compiti derivanti dalla partecipazione alle attività di cooperazione fra autorità di protezione di dati dell'Unione europea (art. 29). Al fine della necessaria ripartizione tra le diverse qualifiche e della conseguente rideterminazione della pianta organica, il predetto incremento di organico è stato recepito con deliberazione del Garante 5 aprile 2018, n. 210 (in GU S.G. 27 aprile 2018, n. 97).

Particolare attenzione è stata riservata, anche nel 2017, all'attività formativa del personale. Con riferimento agli adempimenti previsti dal d.lgs. n. 81/2008 in materia di tutela della salute e della sicurezza nei luoghi di lavoro, sono stati espletati tutti i corsi previsti dalla predetta normativa a favore dei dipendenti.

Allo scopo di migliorare la gestione dei *database*, è stato organizzato un corso interno di aggiornamento in materia di *storage* e gestione delle informazioni, seguito con molto interesse e grande partecipazione.

Inoltre, in seguito ad una procedura comparativa effettuata sul Mepa, l'Autorità ha erogato 6 corsi di formazione di lingua inglese (due di livello avanzato, tre di livello intermedio e uno di livello *legal*).

25

L'attività della Segreteria generale

Complessivamente, nel corso dell'anno sono state somministrate circa 155 ore di formazione non obbligatoria, che hanno interessato circa il 50% del personale.

Presso l'Autorità opera il servizio di controllo interno, 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.

Nel periodo di riferimento, l'attività del Garante è stata improntata al metodo della programmazione e sul rispetto dei principi di economicità ed efficienza dell'azione amministrativa, in conformità al Regolamento n. 1/2000 sull'organizzazione e il funzionamento dell'Ufficio, attraverso l'attività di coordinamento svolta dal Segretario generale, soggetto preposto all'Ufficio ai sensi dell'art. 156, comma 1, del Codice.

Il corretto espletamento da parte del Garante dei compiti e dei poteri attribuiti dalla disciplina vigente è stato garantito dal Segretario generale attraverso il raccordo tra le Unità organizzative e il Collegio, la costante attività istruttoria degli schemi di provvedimento oggetto di esame nel corso di circa cinquanta adunanze, la partecipazione a diversi incontri e innumerevoli interlocuzioni con attori istituzionali e organismi rappresentativi di varie categorie, svolti anche in ambito internazionale ed europeo. Ciò ha consentito, da un lato, di mettere a disposizione, in consessi istituzionali internazionali, l'esperienza maturata del Garante, anche allo scopo di consolidare il proprio orientamento sulle tematiche di maggiore criticità in relazione alla protezione dei dati personali; dall'altro, il costante confronto e l'aggiornamento hanno permesso di riportare nell'Ufficio le migliori buone prassi sviluppate all'estero.

Tra i principali ambiti di intervento, si evidenzia oltre all'attività divulgativa espletata dal Garante in relazione all'applicazione del RGPD, i contatti intercorsi, sempre nella persona del Segretario generale, con Anac e il Dipartimento della funzione pubblica nell'ambito del monitoraggio effettuato sul rispetto del d.lgs. n. 33/2013 presso i soggetti pubblici; le iniziative intraprese per attuare efficacemente i nuovi compiti in materia di cyberbullismo attribuiti al Garante dalla l. n. 71/2017 attraverso gli incontri effettuati con i principali *stakeholders* (Facebook*, Save the children,* Corecom), nonché con la Polizia di Stato (che hanno dato avvio a numerose interlocuzioni per la sottoscrizione di un protocollo di intesa volto a rafforzare il sistema di tutele dai pericoli del web nei confronti dei minori). Di analoga rilevanza, è il contributo fornito dal Garante ai lavori per l'istituzione del *Fintech innovation hub* presso il Ministero dell'economia e delle finanze e le interlocuzioni intercorse con il Ministero della giustizia sulla nuova disciplina in materia di intercettazioni.

Inoltre, la posizione del Garante è stata rappresentata dal Segretario generale in occasione di incontri, convegni e seminari aventi ad oggetto gli aspetti di maggiore criticità interpretativa e/o difficoltà applicativa emergenti dalla disciplina. Gli interventi hanno riguardato, fra i tanti, s*mart* TV e *big data*; *e-privacy*; *fake news*; intelligenza artificiale; *marketing* sul web; *cybersecurity*; minori e *social media*; trasparenza amministrativa.

Al fine di assicurare l'efficienza del Garante, sotto il profilo organizzativo, il Segretario generale ha avviato le necessarie attività volte a definire l'organizzazione dell'Ufficio in vista della applicazione del RGPD, provvedendo altresì a gestire le problematiche riguardanti il personale, le risorse interne e strumentali, la contrattualistica e i rapporti con le altre autorità indipendenti nel quadro delle convenzioni stipulate sui servizi strumentali.

L'efficienza dell'Autorità è stata perseguita anche attraverso il controllo di

gestione, che ha comportato un'analisi periodica degli affari assegnati alle diverse Unità organizzative, con la produzione di una reportistica mensile di carattere statistico, che si è focalizzata sull'andamento nella trattazione degli affari, il riepilogo dei flussi (fascicoli assegnati ed evasi) e il controllo delle pratiche esposte al rischio di arretrato.

Nel 2107 l'Ufficio ha continuato a seguire le attività dell'organo collegiale, e con specifico riguardo alla predisposizione e distribuzione della documentazione necessaria per le adunanze (in particolare schemi di provvedimento, appunti e note), la conservazione dei verbali delle riunioni e degli originali delle deliberazioni adottate nonché del materiale utile per la pubblicazione in Gazzetta ufficiale.

Il Servizio di segreteria del Collegio ha garantito il controllo puntuale dei testi deliberati dal Collegio prima dell'invio alla redazione web per la pubblicazione sul sito istituzionale dell'Autorità, come previsto dalla normativa in materia di trasparenza.

L'Ufficio in un'ottica di efficientamento delle risorse e di maggiore celerità delle attività, nel corso dell'anno ha continuato ad utilizzare modalità di trasmissione elettronica dei documenti predisposti per l'esame e l'approvazione da parte del Collegio, assicurando tempestività ed efficienza nonché risparmio in termini di costi, conformemente a quanto disposto dall'art. 15 del Regolamento n. 1/2000. In tale ambito l'attività svolta consentirà di poter conformare in breve tempo le attività della segreteria del Collegio alle indicazioni contenute nel decreto legislativo n. 217/2017 che ha modificato il Cad.

Il Servizio di segreteria del Collegio ha contribuito a gestire le richieste di oscuramento e di deindicizzazione di alcuni atti dell'Autorità, formulati da interessati e da titolari del trattamento coinvolti a vario titolo in alcune istruttorie dell'Autorità, con particolare riferimento a esigenze di riservatezza riguardo a casi di segreto industriale o *know-how* tecnologico.

25.4. *"Autorità trasparente" e adempimenti relativi alla disciplina anticorruzione*

Nel 2017 è stato adottato il primo Piano triennale di prevenzione della corruzione (Ptpc) per gli anni 2017-2019 redatto in conformità agli obiettivi programmatici indicati dal Garante (doc. web n. 5977598) e pubblicato sul sito istituzionale nella sezione Autorità trasparente (doc. web n. 591436). Le misure generali e specifiche di prevenzione della corruzione previste dal Piano sono state attuate nel rispetto delle previsioni ivi contenute.

Fra l'altro, particolare attenzione è stata riservata all'informazione e alla formazione del personale, al quale è stato trasmesso il testo integrale del citato Piano con i relativi allegati, nonché copia del testo del codice etico, richiamando l'attenzione sulle misure contenute e invitando a segnalare al proprio dirigente eventuali situazioni di possibile illecito nonché di personale conflitto di interessi. Avvalendosi poi dell'offerta formativa della Scuola nazionale dell'amministrazione, unità di personale operante in aree più esposte al rischio di corruzione ha frequentato, in una logica di progressivo coinvolgimento del personale secondo un criterio di rotazione, un corso specialistico dedicato alla prevenzione della corruzione e trasparenza.

Un'importante misura del Piano ha riguardato gli adempimenti in materia di trasparenza ed in particolare l'aggiornamento della struttura della sezione Autorità trasparente, la quale è stata integrata anche con riferimento ai "dati ulteriori" ed ai moduli per l'esercizio del diritto di accesso civico, che sono stati aggiornati nei loro contenuti. A tale riguardo, si evidenzia che al Responsabile della prevenzione della

corruzione e della trasparenza (Rpct) sono pervenute trenta istanze di riesame, rispetto a richieste di accesso civico presentate presso gli Uffici del Garante, alle quali il Responsabile ha dato puntuale riscontro nel termine previsto di venti giorni (art. 5, comma 7, d.lgs. n. 33/2013), e due istanze di accesso civico relative a dati a pubblicazione obbligatoria (art. 5, comma 1, d.lgs. n. 33/2013) che non hanno dato luogo ad un adeguamento perché i dati risultavano già pubblicati o non sussisteva il relativo obbligo.

Con riguardo alla misura concernente la rotazione degli incarichi dirigenziali si è verificato che tale misura – strutturalmente già prevista dall'art. 9, comma 2, Regolamento n. 1/2000 del Garante – è stata osservata presso il Garante quanto agli incarichi in essere nell'anno 2017, fatti salvi i soli casi di motivata esclusione indicati nel Ptpc 2017-2019.

Sono state predisposte e pubblicate sul sito del Garante sia la relazione annuale del Rpct (doc. web n. 7611100) per l'anno 2017 (art. 1, comma 14, l. n. 190/2012) relativa all'efficacia delle misure di prevenzione definite nel Piano triennale di prevenzione della corruzione 2017-2019 sia, nel rispetto del termine del termine del 30 aprile 2017, la griglia di rilevazione di cui all'allegato 2 della delibera Anac n. 236 del 2017, che il Rpct è tenuto a pubblicare in assenza di Oiv o strutture equivalenti presso l'Autorità.

Sempre in materia di trasparenza è stato inoltre fornito costante supporto a tutti gli uffici chiamati ad adempiere ad obblighi di pubblicazione.

25.5. *Il settore informatico e tecnologico*

Sviluppo del sistema informativo e dei servizi ICT

Nel 2017 è proseguita l'attività di sviluppo del sistema informativo con la scelta di un nuovo sistema di gestione del protocollo informatico che si integri con un sistema di *workflow* a supporto, *in primis*, dell'attività amministrativa ma, in prospettiva e più in generale, a disposizione per la documentazione automatica delle attività lavorative interne.

Dal punto di vista infrastrutturale non sono state compiute operazioni rilevanti poiché la future evoluzioni del sistema informativo terranno in debito conto i percorsi individuati dal Cad, in favore di un progressivo trasferimento degli *asset* infrastrutturali su servizi *cloud* predisposti per le pp.aa. e di una concentrazione delle competenze e delle risorse interne sui temi del miglioramento dei servizi applicativi.

Sicurezza informatica dell'Ufficio

Nel 2017 nessun evento relativo alla sicurezza ha prodotto danni o disservizi nel dominio dell'Ufficio. Non si sono registrate situazioni pregiudizievoli rispetto alla sicurezza informatica sulle postazioni individuali e sui sistemi *server*, né su altre componenti dell'infrastruttura.

La continuità dei servizi accessibili al pubblico (notificazione dei trattamenti e richieste di verifiche preliminari per gli istituti bancari) è stata in linea con i valori di *downtime* dei servizi ancora gestiti *on premises* intorno alle otto ore complessive nell'arco dell'anno, dovuti principalmente a guasti sulla rete elettrica.

Attività di consulenza e cooperazione interna ed esterne

Le unità organizzative dell'Ufficio hanno cooperato assiduamente attraverso azioni di supporto e consulenza interna sulle tematiche di comune interesse e in base alle rispettive competenze: significativa in questo senso, in particolare, l'interazione con la componente tecnologica dell'Ufficio sui temi connessi all'innovazione digitale e alla sicurezza informatica, sia nell'ambito della trattazione di affari e procedimenti sia nel contesto dell'attività ispettiva e internazionale.

In tal senso, si menziona l'impegno nel supporto tecnologico alla campagna

ispettiva sul *telemarketing*, che ha comportato lo svolgimento di accertamenti anche all'estero (*extra* UE) e l'analisi di copiose moli di dati su chiamate indesiderate che ha consentito di rilevare e mettere a fuoco numerose irregolarità da parte di operatori di comunicazione elettronica poi oggetto di sanzioni nonché il contributo fornito all'*audit* periodico nei confronti del sistema nazionale di informazione visti (VIS), di cui alla decisione del Consiglio 2004/512/CE, finalizzato alla vigilanza sulla legittimità del trattamento dei dati personali dei richiedenti il visto.

In sede di resa dei previsti pareri da parte dell'Autorità, la componente tecnologica dell'Ufficio ha contribuito alla definizione del quadro attuativo del Cad e, per quanto riguarda lo sviluppo delle nuove tecnologie in ambito pubblico, ha fornito consulenza relativamente alle banche dati di interesse nazionale, specialmente in relazione all'anagrafe tributaria, all'Anpr e alla sanità.

Infine, si menziona la partecipazione agli impegni internazionali, in particolare nell'ambito del sottogruppo *technology* del Gruppo Art. 29 e dell'*International Working Group on Data Protection in Telecommunications* (IWGDPT) (cfr. par. 22.4).

Si evidenzia il ruolo di relatore che l'Autorità italiana ha svolto in vari pareri resi dal *Working Party* per la corretta interpretazione del RGPD e, segnatamente, il parere in materia di portabilità dei dati e quello sui trattamenti di dati personali in contesti lavorativi. Nell'ambito dell'IWGDPT, l'Autorità si è fatta promotrice di un'azione di sensibilizzazione in materia di cyberbullismo, con particolare riguardo alle concrete possibilità tecniche di individuare con prontezza e rimuovere contenuti offensivi dai siti web. Il tema è stato oggetto di attenzione da parte delle altre Autorità europee, di quelle dei Paesi *extra* UE riuniti nel Gruppo, nonché dell'OECD, membro del Gruppo, che recepirà tali indicazioni nelle proprie linee guida.

L'Autorità si è impegnata nelle annuali attività di supervisione sui trattamenti di dati personali effettuati dalle agenzie europee Europol e Eurojust, con particolare riguardo agli aspetti legati alle misure di sicurezza e ha collaborato nei tavoli di lavoro internazionali istituiti per la riforma del quadro giuridico europeo in materia di comunicazioni elettroniche (nuovo regolamento *e-Privacy*) e per la definizione di linee guida in materia di rischi dei trattamenti e misure di sicurezza (European Union Agency for Network and Information Security – Enisa, *Working group on security of personal data processing*).

I dati statistici

IV - I dati statistici 2017

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	573
Pareri a Presidenza del Consiglio dei ministri e ministeri (art. 154, comma 4, del Codice)	19
Pareri a Presidenza del Consiglio dei ministri e ministeri su norme di rango primario	5
Pareri ai sensi dell'art. 5, comma 7, d.lgs. n. 33/2013	38
Autorizzazioni individuali al trattamento dei dati sensibili e giudiziari (art. 41 del Codice)	5
Provvedimenti concernenti trasferimenti di dati consentiti verso Paesi terzi (art. 44, comma 1, lett. *a*), del Codice)	14
Decisioni su ricorso (art. 145 del Codice)	276
Provvedimenti collegiali su segnalazioni e reclami (artt. 142-144 del Codice) nonché a seguito di accertamenti d'ufficio (art. 154 del Codice) e ai sensi degli artt. 10, comma 2, 13, comma 5, lett. *c*), e 150, comma 5, del Codice	42
Ordinanze-ingiunzione adottate dal Garante	116
Riscontri a segnalazioni, reclami, richieste di parere e quesiti (artt. 142-144 del Codice e artt. 5 e 11, Reg. Garante n. 1/2007)	5.819
Provvedimenti collegiali su verifiche preliminari per trattamenti che presentano rischi specifici (art. 17 del Codice)	26
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)	1
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari (art. 154, comma 1, lett. *l*), del Codice)	3
Ulteriori pareri resi a soggetti pubblici ai sensi dell'art. 154, comma 1, lett. *g*), del Codice	5
Risposte ad atti di sindacato ispettivo e di controllo	1
Risposte a quesiti e altre istanze	16.193
Leggi regionali esaminate	8
Rilievi formulati in relazione a leggi regionali ai fini dell'impugnazione ex art. 127 Cost.	6
Accertamenti e controlli efffettuati *in loco* (artt. 157-158 del Codice)	275
Violazioni amministrative contestate	589
Sanzioni applicate con ordinanza ingiunzione	1.261
Pagamenti derivanti dall'attività sanzionatoria	€ 3.776.694
Comunicazioni di notizia di reato all'autorità giudiziaria	41
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	4
Ricorsi (trattati) ex art. 152 del Codice	14
Opposizioni (trattate) a provvedimenti del Garante	73
Notificazioni pervenute nell'anno 2017	3.179
Notificazioni pervenute dal 2004 al 31 dicembre 2017	32.238
Riunioni del Gruppo Art. 29	5
Partecipazione a sottogruppi di lavoro - Gruppo Art. 29	46
Riunioni autorità comuni di controllo (Europol, SIS II, Dogane, Eurodac, VIS)	15
Conferenze internazionali	2
Riunioni presso il CoE, OCSE e altri organismi internazionali	14
Riunioni e *workshop* presso Consiglio/Commissione e altri organismi UE	12
Quesiti, questionari e richieste di contributi provenienti da altre Autorità e Istituzioni	27

Tabella 1. Sintesi delle principali attività dell'Autorità

Attività di comunicazione dell'Autorità	
Comunicati stampa	41
Newsletter	13
Bollettino radiofonico del Garante	18
Prodotti editoriali	4
Prodotti web	17

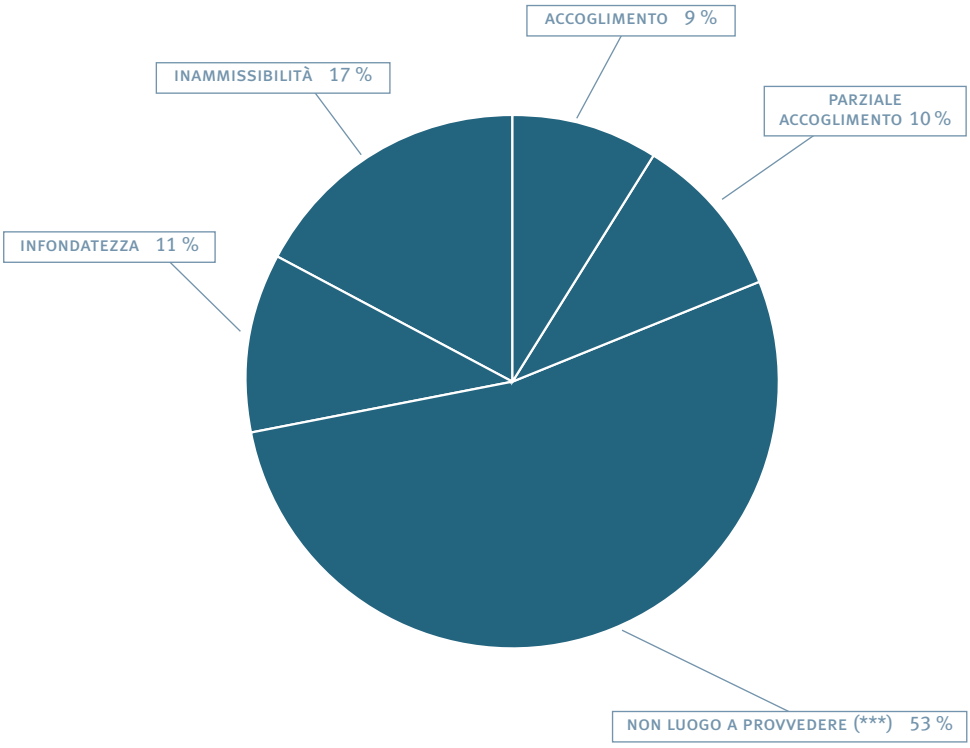
Tabella 2. Attività di comunicazione dell'Autorità

Tabella 3. Pareri ex art. 154, comma 4, del Codice

Pareri ex art. 154, comma 4, del Codice	
Temi	Riscontri resi nell'anno (*)
Attività di polizia, sicurezza nazionale e governo del territorio	5
Giustizia	1
Dati sanitari	3
Fisco	5
Carta elettronica studenti	1
Istruzione	1
Registro pubblico delle opposizioni	1
Previdenza - Ape	1
Codice della navigazione	1
Totale	19

Tabella 4. Tipologia delle decisioni su ricorsi

Decisioni su ricorsi	
Tipi di decisione (**)	Numero ricorsi
Accoglimento	24
Parziale accoglimento	28
Non luogo a provvedere (***)	147
Infondatezza	30
Inammissibilità	47
Totale	276



(*) Inerenti anche ad affari pervenuti anteriormente al 2017
(**) 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

Tabella 5. Suddivisione dei ricorsi in relazione alle categorie di titolari del trattamento

Categorie di titolari	
	Numero ricorsi
Banche e società finanziarie	34
Compagnie di assicurazione	6
Sistemi di informazioni creditizie	7
Centrale rischi Banca d'Italia e trattamenti presso archivio Cai	3
Società di informazioni commerciali	5
Amministrazioni pubbliche e concessionari di pubblici servizi	44
Strutture sanitarie pubbliche e private	13
Fornitori telefonici e telematici	16
Attività di *marketing* svolta da imprenditori privati	19
Datori di lavoro pubblici e privati	29
Editori (anche televisivi)	81
Liberi professionisti	6
Amministrazioni condominiali	3
Associazioni	4
Altro	6
Totale	27

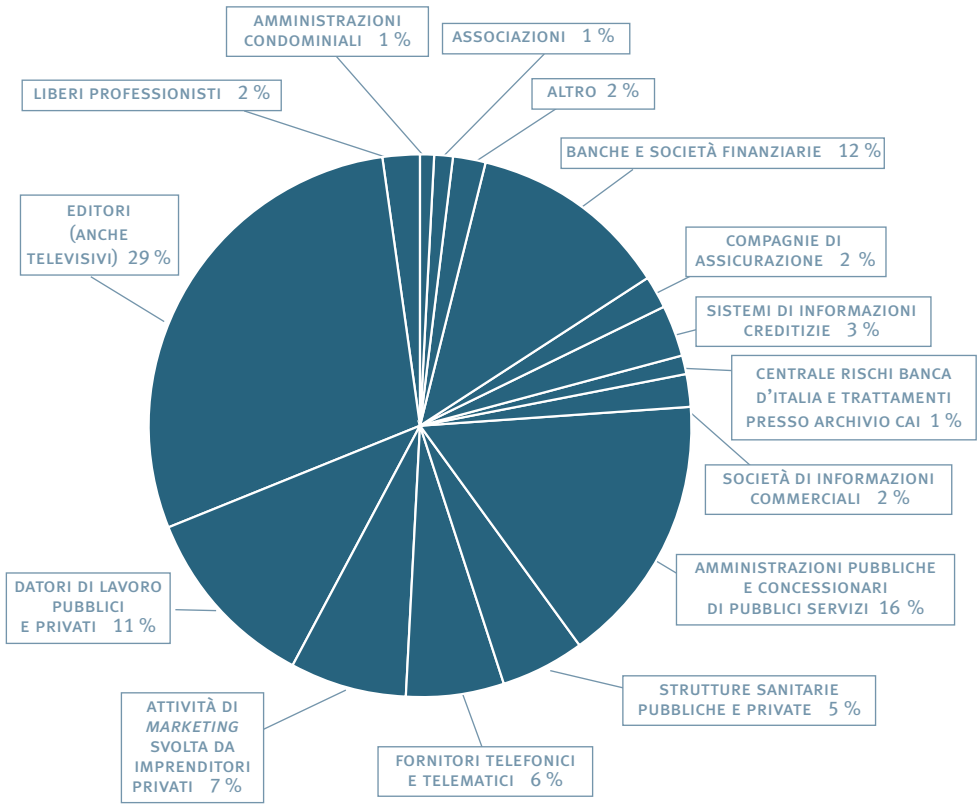
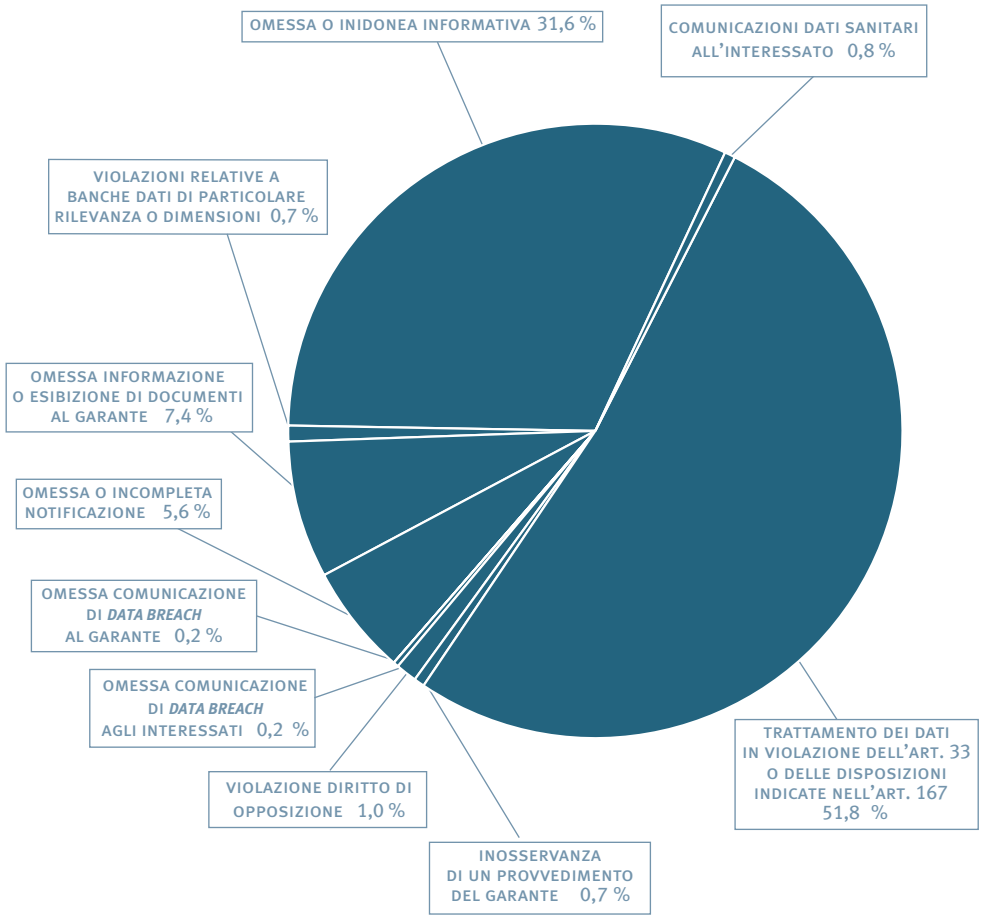


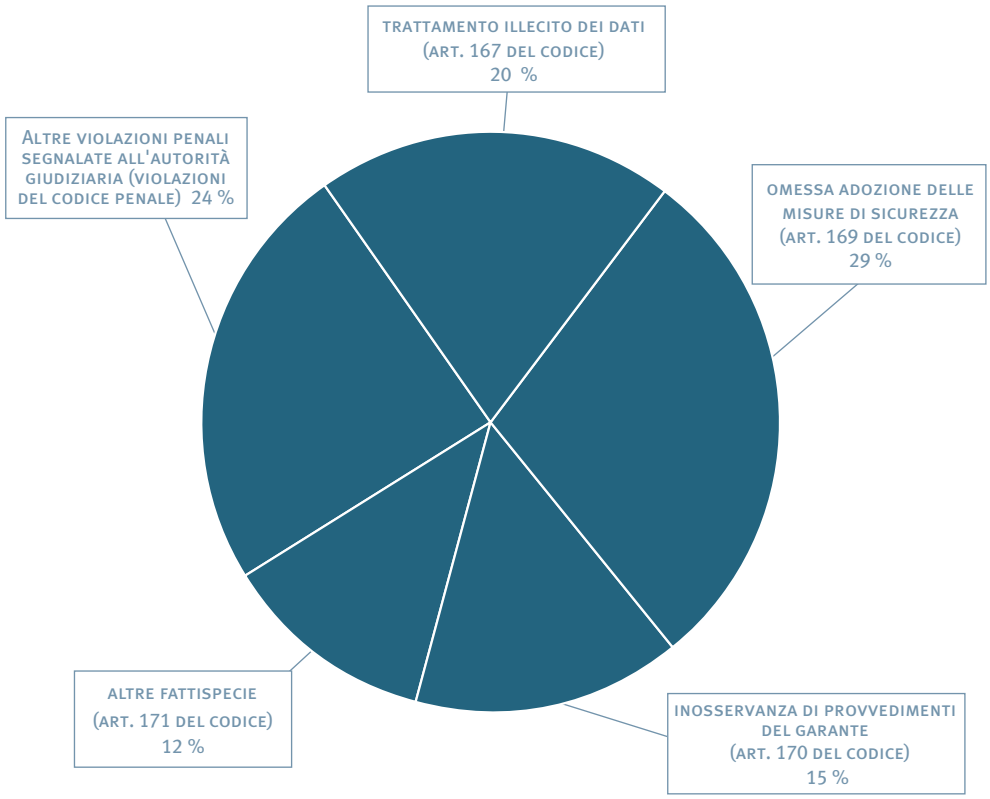
Tabella 6. Violazioni amministrative contestate

Violazioni amministrative contestate	
Omessa o inidonea informativa (art. 161 del Codice)	186
Violazione delle modalità di comunicazione di dati sanitari all'interessato (art. 162, comma 2, del Codice)	5
Trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis*, del Codice)	305
Inosservanza di un provvedimento del Garante (art. 162, comma 2-*ter*, del Codice)	4
Violazione del diritto di opposizione (art. 162, comma 2-*quater*, del Codice)	6
Omessa comunicazione di eventi di *data breach* al Garante (art. 162-*ter*, comma 1, del Codice)	1
Omessa comunicazione di eventi di *data breach* agli interessati (art. 162-*ter*, comma 2, del Codice)	1
Omessa o incompleta notificazione (art. 163 del Codice)	33
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)	44
Violazioni relative a banche dati di particolare rilevanza o dimensioni (art. 164-*bis*, comma 2, del Codice)	4
Totale	**589**



Comunicazioni di notizia di reato all'autorità giudiziaria	
	Segnalazioni
Trattamento illecito dei dati (art. 167 del Codice)	8
Omessa adozione delle misure di sicurezza (art. 169 del Codice)	12
Inosservanza di provvedimenti del Garante (art. 170 del Codice)	6
Altre fattispecie (art. 171 del Codice)	5
Altre violazioni penali segnalate all'autorità giudiziaria (violazioni del codice penale)	10
Totale	41

Tabella 7. Comunicazioni di notizia di reato all'autorità giudiziaria



Pagamenti derivanti dall'attività sanzionatoria	
Somme versate a titolo di oblazione in via breve	1.385.500
Somme versate in conseguenza di ordinanze ingiunzione	1.329.590
Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169 del Codice)	180.000
Ulteriori entrate derivanti dall'attività sanzionatoria	881.604
Totale	**3.776.694**

Tabella 8. Pagamenti derivanti dall'attività sanzionatoria

Quesiti		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale quesiti	**526**	**400**

Tabella 9. Quesiti

(*) Inerenti anche ad affari pervenuti anteriormente al 2017

Tabella 10. Segnalazioni e reclami

Segnalazioni e reclami		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale segnalazioni e reclami	**5.708**	**5.419**
Temi principali		
Assicurazioni	56	45
Associazioni	36	29
Centrali rischi	124	118
Concessionari pubblici servizi	89	40
Condominio	35	27
Credito	240	192
Enti locali	113	113
Imprese	164	105
Informazioni commerciali	12	12
Istruzione	34	34
Lavoro	210	235
Marketing (posta cartacea, *e-mail*, fax, sms)	225	101
Marketing telefonico	2.127	2.786
Recupero crediti	104	93
Sanità e servizi di assistenza sociale	110	110
Tributi	48	48
Videosorveglianza	296	198

Tabella 11. Atti di sindacato ispettivo e controllo

Atti di sindacato ispettivo e controllo	
Temi	Numero
Pubblicità beneficiari finanziamenti fondi europei FEAGA-FEASR	1
Totale	**1**

Tabella 12. Tipologie di notificazioni pervenute: 2004-2017

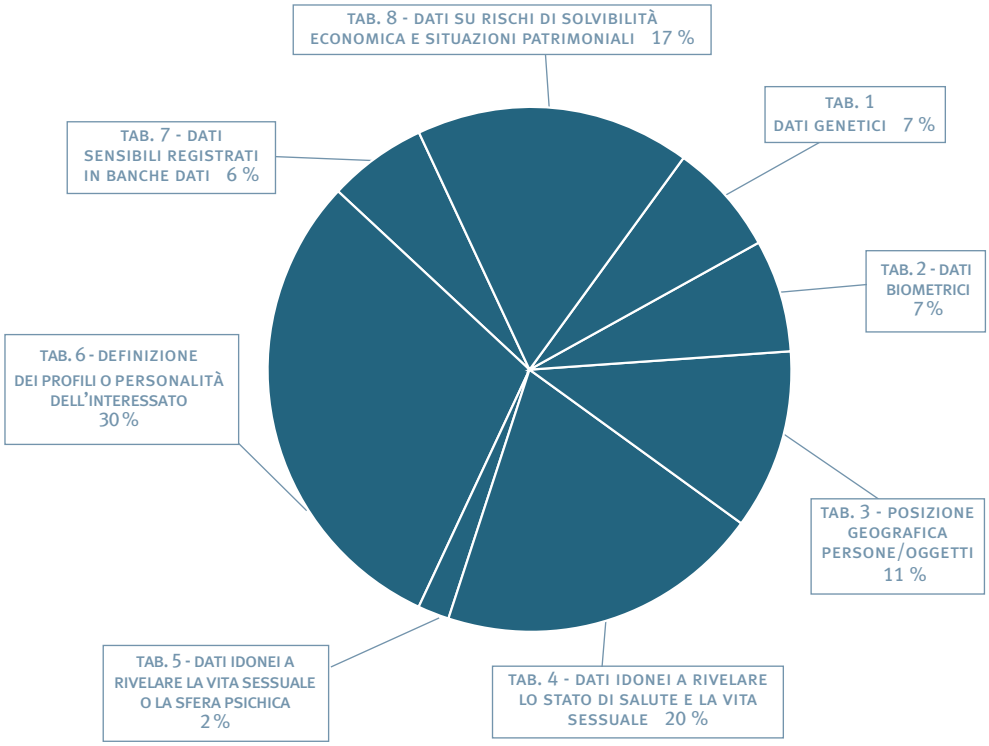
Tipologie di notificazioni pervenute: 2004-2017 (**)			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute (**)
Prima notificazione al Garante	1.366	23.800	25.166
Modifica di una precedente notificazione	228	5.325	5.553
Notificazione della cessazione del trattamento	126	1.393	1.519
Totale	**1.720**	**30.518**	**32.238**

(*) Inerenti anche ad affari pervenuti anteriormente al 2017

(**) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2017

Suddivisione delle notificazioni per tipologia di trattamento effettuato 2004-2017	
Tabelle di notificazione compilate (*)	Numero
Tabella 1 - Trattamento di dati genetici	3.302
Tabella 2 - Trattamento di dati biometrici	3.211
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	5.455
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	8.929
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	910
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	14.897
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	2.500
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	7.673
Totale (**)	**46.877**

Tabella 13. Suddivisione delle notificazioni per tipologia di trattamento effettuato 2004-2017



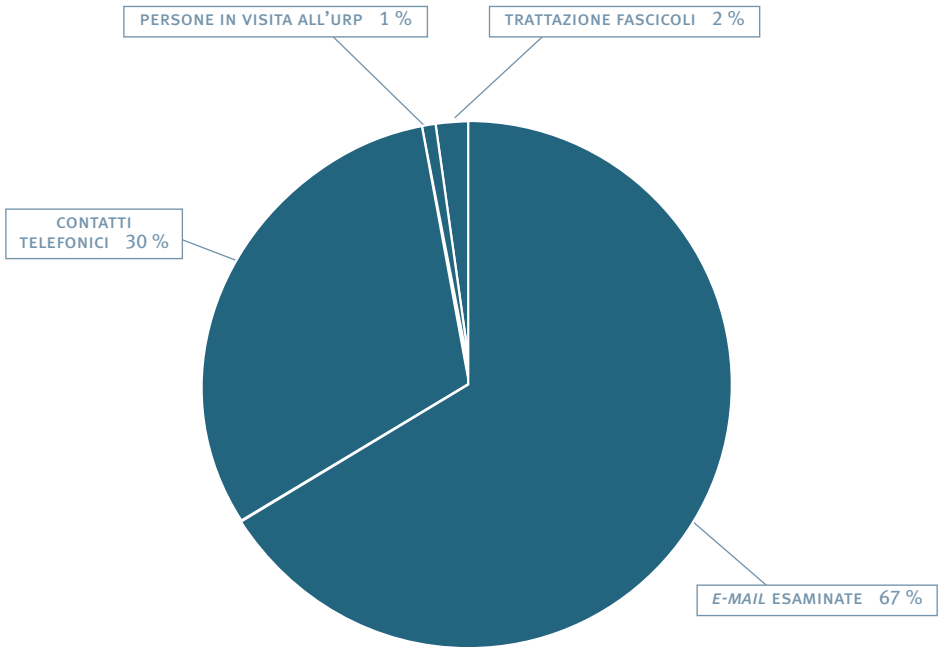
(*) Situazione alla data del 31 dicembre 2017
(**) N.B. Il totale è superiore a quello della precedente tabella in quanto una singola notificazione può riguardare più trattamenti

Tabella 14. Tipologie di notificazioni pervenute nel 2017

Tipologie di notificazioni pervenute nel 2017 (*)			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute (*)
Prima notificazione al Garante	60	2.480	2.540
Modifica di una precedente notificazione	19	492	511
Notificazione della cessazione del trattamento	9	119	128
Totale	**88**	**3.091**	**3.179**

Tabella 15. Ufficio relazioni con il pubblico

Ufficio relazioni con il pubblico	
	2017
E-mail esaminate	10.838
Contatti telefonici	4.869
Persone in visita all'Urp	187
Trattazione pratiche relative a fascicoli	299
Totale	**16.193**



(*) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2017

Grafico 16. *E-mail* esaminate dall'Ufficio relazioni con il pubblico

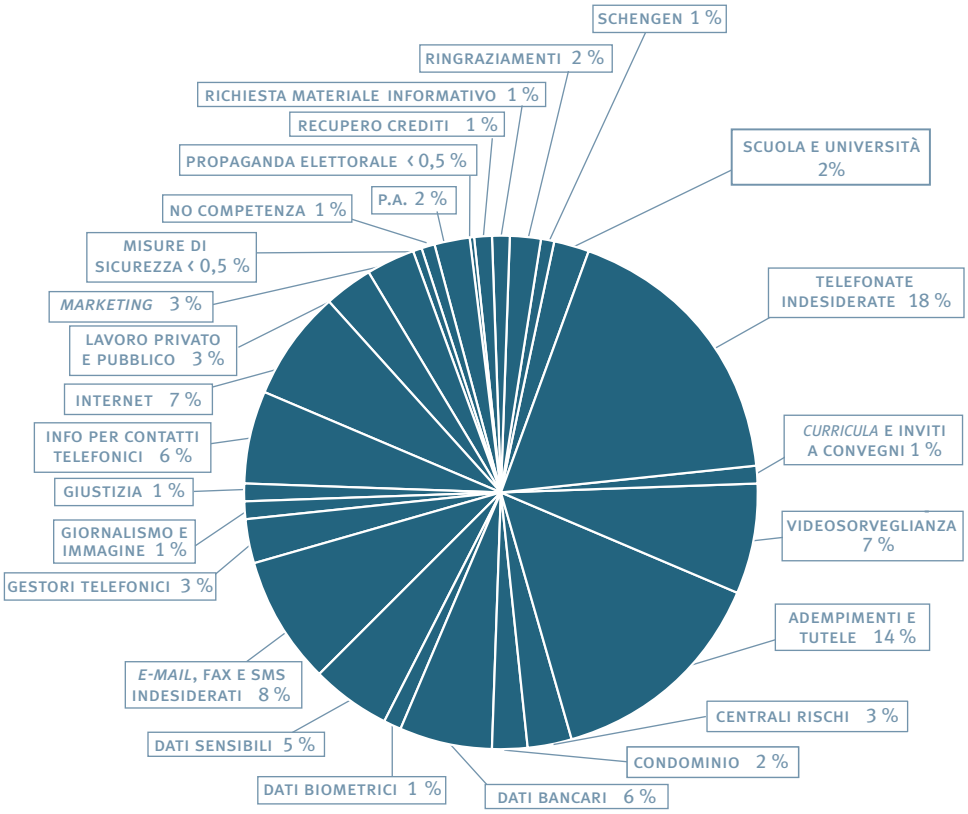


Tabella 17. Posti previsti in organico (*)

Posti previsti in organico	
Segretario generale	1
Dirigenti	21
Funzionari	88
Operativi	26
Esecutivi	1
Totale	137
Personale a contratto	8

(*) Con l. 20 novembre 2017, n. 167 è stato introdotto un incremento del ruolo organico in misura pari a 25 unità, recepito con deliberazione del Garante del 5 aprile 2018, n. 210 (in GU S.G. 27 aprile 2018, n. 97)

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	75	4	3	76
Operativi	24			24
Esecutivi	–	–	–	–
Totali	**113**	**6**	**3**	**116**
Personale a contratto				8

Tabella 19. Risorse finanziarie

Risorse finanziarie		
ENTRATE	**SOMME ACCERTATE**	
	ANNO 2017	**ANNO 2016**
ENTRATE CORRENTI	**21.061.841,95**	**19.889.832,13**
Trasferimenti da altre Autorità	0,00	10.000.000,00
Trasferimenti da Mef	20.287.821,00	9.326.540,00
Diritti di segreteria ed altri proventi	774.020,95	563.292,13
Partite di giro	**5.705.454,27**	**5.399.894,16**
TOTALE ENTRATE	**26.767.296,22**	**25.289.726,29**
USCITE	**SOMME IMPEGNATE**	
	ANNO 2017	**ANNO 2016**
USCITE CORRENTI	**19.168.598,05**	**18.955.899,30**
Personale e oneri connessi	15.095.403,48	14.656.353,30
Acquisto di beni e servizi ed indennità di carica	3.598.143,03	3.777.607,02
Versamenti al bilancio dello Stato	251.735,36	253.611,80
Trasferimenti ed altri oneri	223.316,18	268.327,18
USCITE IN CONTO CAPITALE	**259.305,33**	**138.640,00**
Immobilizzazioni materiali e immateriali	259.305,33	138.640,00
Partite di giro	**5.705.454,27**	**5.399.894,16**
Avanzo di amministrazione	1.633.938,57	795.292,83
TOTALE USCITE	**26.767.296,22**	**25.289.726,29**

Valori: euro

(*) Situazione alla data del 31 dicembre 2017

Tabella 20. Attività internazionali dell'Autorità

Unione europea			
Gruppo Articolo 29	Sessione plenaria Art. 29		7 e 8 febbraio 4 e 5 aprile 7 e 8 giugno 3 e 4 ottobre 28 e 29 novembre
	Riunioni dei sottogruppi	*Border Travel Law Enforcement* (BTLE)	17 gennaio 9 marzo 16 maggio 5 settembre 26 ottobre
		Cooperation	11 gennaio 7 marzo 3 maggio 3 e 4 luglio 19 e 20 ottobre
		E-Government	2 febbraio 3 marzo 17 maggio 24 ottobre
		Financial Matters	1° febbraio 16 marzo 5 luglio 17 ottobre
		Future of Privacy	27 gennaio 17 marzo 23 maggio 12 settembre 7 novembre
		Key Provisions	23 febbraio 4 maggio 27 giugno 19 ottobre
		International Transfers	5 gennaio 13 e 14 marzo 4 e 5 maggio 18 e 19 giugno 16 e 17 ottobre
		Technology	18 e 19 gennaio 8 e 9 marzo 15 e 16 maggio 6 e 7 settembre 25 e 26 ottobre
		EDPB IT Task Force	1° febbraio 4 maggio 6 settembre 7 e 8 dicembre
		Enforcement	24 gennaio 15 marzo 7 luglio (*workshop*) 27 ottobre
	Riunioni dei gruppi *ad hoc*	*Workshop on WP29 communication*	1° giugno

Unione europea	
Autorità di controllo comune Europol	23-26 gennaio (ispezione) 19 e 20 aprile 6 aprile (incontro con Europol) 21 e 22 marzo (NPG *meeting*) 11-15 dicembre (ispezione)
Europol Cooperation Board	16 giugno 16 novembre
Autorità di controllo comune Dogane	20 aprile
Gruppo di coordinamento della supervisione SID	20 aprile
Gruppo di coordinamento della supervisione SIS II	13 giugno 14 novembre
Gruppo di coordinamento della supervisione Eurodac	14 giugno 15 novembre
Gruppo di coordinamento della supervisione VIS	13 giugno 15 novembre

Unione europea	
Riunioni di gruppi di esperti	
Workshop on Consumer Protection (CPC)	23 marzo
ENISA *expert Group*	4 aprile 19 giugno 22 settembre
ENISA *Privacy Forum/IPEN workshop*	7-9 giugno
C- ITS *Intelligent Transport System WG*	21 febbraio 13 giugno 24 ottobre
LIBE *Hearing e-Privacy Regulation*	11 aprile
Chief Information Officers Meeting	15 giugno
Expert meeting on broadening law enforcement access to centralised bank account registries	25 e 26 ottobre
EMA – *Anonymisation Expert Group*	29 novembre - 1° dicembre

Altri *forum* internazionali		
Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	**Comitato WPSPDE *"Working Party on Security and Privacy in the Digital Economy"* - *Bureau* e Plenaria**	12 e 13 maggio (*workshop* MADE) 15-17 maggio 2 ottobre (*workshop*)
Consiglio d'Europa	**Comitato Consultivo Convenzione 108/1981 (T-PD)**	19-21 giugno 22-24 novembre
	T-PD *Bureau*	29-31 marzo 11-13 settembre 18-20 dicembre
	CAHENF	6 e 7 febbraio 2-4 maggio 21 e 22 settembre
Gruppi di lavoro specifici	**Gruppo internazionale di lavoro sulla protezione dei dati nelle telecomunicazioni (IWGDPT)**	24 e 25 aprile 27 e 28 novembre
International Enforcement	**GPEN *(Global Privacy Enforcement Network)***	17 febbraio (*Sweep conference call*) 20 aprile (*Sweep conference call*) 21 e 22 giugno (*Practitioner event*)

Conferenze internazionali	
Conferenza di primavera delle Autorità europee di protezione dati	27 e 28 aprile, Limassol
38ª Conferenza internazionale delle Autorità di protezione dati	25-29 settembre, Hong Kong

Altre conferenze e *meeting*	
Workshop of National Data Protection Authorities Experts on civil drones applications	12 gennaio, Bruxelles
CEN-CENELEC *Workshop Plenary Meeting Meeting*	16 gennaio, Bruxelles 16 marzo, Bruxelles
Workshop "The EU Charter in the activity of national DPAs"	20 gennaio, Fiesole
***Certification Workshop* – Cnil**	30 marzo, Parigi
CIPL *Dialogue on GDPR implementation and compliance – Workshop*	6-7 marzo, Madrid
***58° meeting* ICANN**	13 e 14 marzo, Copenhagen
FabLab	5-6 aprile, Bruxelles 18 ottobre, Bruxelles
AFME/EBF *Joint Event on "Banks & Data - Managing data protection and the free flow of data*	16 maggio, Bruxelles
Appa *Workshop* – Cnil	18 maggio, Parigi
UEMOA – *International conference on credit reporting*	30 maggio e 1° giugno, Dakar
XXIX *Case Handling Workshop*	20 e 21 giugno, Manchester
Bridge Health-EUBIROD meeting	20-23 settembre, Cipro
20th anniversary of the Oviedo Convention: relevance and challenges	24 e 25 ottobre, Strasburgo
Anonymisation Workshop	4 dicembre, Brdo
Internet Governance Forum	20 dicembre, Ginevra

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Redazione
Garante per la protezione dei dati personali

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

stampa:
Tipolitografia Ugo Quintily S.p.A.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI