1997 2017

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

Relazione2016

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

Antonello Soro, *Presidente*
Augusta Iannini, *Vice Presidente*
Giovanna Bianchi Clerici, *Componente*
Licia Califano, *Componente*

Giuseppe Busia, *Segretario generale*

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 696773785
www.garanteprivacy.it

Relazione2016

www.garanteprivacy.it

I numeri del 2016

Provvedimenti collegiali **561**

277
Ricorsi decisi

122
Ordinanze-ingiunzione

29
Verifiche preliminari

20
Pareri resi al Governo

9
Autorizzazioni generali per i dati sensibili e giudiziari

4.633
Riscontri a segnalazioni e reclami

€ 3.289.896
Sanzioni riscosse

282
Ispezioni

2.339
Sanzioni contestate

2.369
Notificazioni pervenute

53
Comunicazioni all'autorità giudiziaria

24.097 **Risposte a quesiti**

50
Comunicati e *newsletter*

5.019.947
Accessi al sito web

In evidenza – 2016

Gennaio

Abbiamo dichiarato illecito e vietato ad una società la costituzione e la diffusione su un sito web di un elenco telefonico di oltre 12.500.000 persone contenente dati personali (nome e cognome, indirizzo, recapito telefonico, a volte anche riservato, numero di cellulare o indirizzo *e-mail*) non provenienti dal *Data base* unico (DBU) e raccolti senza il consenso degli interessati. I dati erano stati acquisiti in maniera automatica e indiscriminata attraverso *script* "lanciati" direttamente sulle fonti web e in grado di acquisirne i contenuti (cd. web *scraping*) ed erano a disposizione degli utenti del sito della società consentendo la consultabilità *online* delle numerazioni e anche la "ricerca inversa" delle generalità di un abbonato attraverso il numero di telefono. Abbiamo altresì disposto la cancellazione dei dati trattati in modo illecito (doc. web n. 6053915)

Abbiamo autorizzato un ospedale e alcuni centri di cura impegnati in uno studio osservazionale multicentrico a trattare i dati sulla salute dei pazienti in assenza dell'informativa e del consenso, qualora sussistano accertate condizioni che impediscano temporaneamente la prestazione del consenso e tale incapacità non sia riacquisita prima del termine del previsto periodo di *follow up*. Ciò allo scopo di effettuare una ricerca sulle complicanze emorragiche in pazienti in terapia con nuovi farmaci anticoagulanti (doc. web n. 4727402)

Abbiamo ritenuto lecita la diffusione *online* di un articolo giornalistico relativo a vicende sentimentali e giudiziarie di un noto personaggio pubblico che ne aveva chiesto la rimozione da un *blog* contestando l'applicabilità delle disposizioni contenute nel Codice a tutela della manifestazione del pensiero. Nel dichiarare infondato il ricorso, abbiamo invece stabilito che al *blog* si estendono le garanzie riguardanti l'attività giornalistica in quanto strumento di manifestazione del pensiero, anche se non riconducibile a giornalisti professionisti o pubblicisti (doc. web n. 4747581)

Febbraio

Abbiamo sanzionato una società fornitrice di servizi di comunicazione elettronica, a seguito di ispezione, per aver effettuato un trattamento di dati di traffico telefonico, conservandoli per finalità di accertamento e repressione dei reati, senza aver adottato le misure di riconoscimento biometrico per il controllo delle aree ad accesso selezionato e *strong authentication* consistenti nell'uso contestuale di almeno due differenti tecnologie di autenticazione (doc. web n. 5431626)

Abbiamo reso parere favorevole su uno schema di regolamento di una regione concernente la costituzione, la tenuta e il funzionamento del registro tumori regionale (costituito da un archivio informatico di dati personali, privati di elementi identificativi diretti e riferiti ai casi di neoplasia insorti nella popolazione regionale), richiedendo alcune specifiche integrazioni riguardo, in particolare, i titolari e i responsabili del trattamento, gli obblighi e le modalità di trasmissione dei dati e le misure di sicurezza ivi compresa la conservazione separata dei dati anagrafici da quelli sanitari (doc. web n. 4853986)

Abbiamo accolto il ricorso di un utente Facebook nei confronti del *social network* ordinando il blocco del trattamento dei dati del falso *account* (creato da un altro utente, utilizzando fraudolentemente i dati e la fotografia postata sul suo profilo) nonché la comunicazione al ricorrente delle informazioni circa l'origine dei dati, le finalità, le modalità e la logica del trattamento, gli estremi identificativi del titolare e del responsabile, i soggetti o le categorie di soggetti cui i dati sono stati comunicati e la

conservazione dei medesimi dati già trattati per un'eventuale acquisizione da parte dell'autorità giudiziaria. È stata la prima pronuncia dell'Autorità nei confronti del colosso web con la quale ha innanzitutto affermato la propria competenza a intervenire a tutela degli utenti italiani (doc. web n. 4833448)

Abbiamo reso parere favorevole ad uno schema di decreto del Ministero dei beni e delle attività culturali e del turismo concernente la realizzazione di una banca dati dei beni culturali illecitamente sottratti. Considerata la natura dei dati raccolti e la finalità del trattamento funzionale ad attività di polizia, abbiamo subordinato il parere alla natura regolamentare dell'atto e all'inserimento di ulteriori indicazioni quali, in particolare, una specifica previsione relativa alla comunicazione dei dati personali contenuti nella banca dati ad altre autorità italiane ed europee, nonché all'eventuale trasferimento di tali dati ad autorità competenti di Paesi terzi (doc. web n. 4727696)

Marzo

Abbiamo condizionato il parere favorevole su uno schema di decreto legislativo concernente la revisione e la semplificazione delle disposizioni di prevenzione della corruzione, pubblicità e trasparenza ad alcune precisazioni allo scopo di garantire maggiori tutele per i cittadini. Abbiamo chiesto, tra l'altro, di razionalizzare e rimodulare gli obblighi di pubblicazione in funzione del grado di esposizione al rischio corruttivo, dell'effettiva necessità di conoscenza da parte dei cittadini e del bilanciamento delle esigenze di trasparenza con il diritto alla protezione dei dati; di precisare con maggiore dettaglio l'estensione degli obblighi di trasparenza e osservare una maggiore proporzionalità negli obblighi di pubblicazione dei dati patrimoniali per il personale pubblico (doc. web n. 4772830)

Abbiamo sanzionato un consulente tecnico dell'autorità giudiziaria che aveva duplicato un *database*, alimentato costantemente da informazioni personali (dati di traffico telefonico o relativi a utenze telefoniche e dati giudiziari) acquisite lecitamente in ragione degli incarichi consulenziali o peritali ricoperti. La duplicazione e organizzazione autonoma della banca dati ha comportato in capo al consulente la veste di soggetto privato titolare del trattamento ed, in quanto tale, è stato sanzionato per avere utilizzato e conservato, oltre i termini di conclusione dell'incarico, banche dati di grandi dimensioni in violazione delle norme in tema di informativa, consenso e autorizzazione del Garante (doc. web. n. 4858951)

A seguito di una segnalazione, abbiamo dichiarato illecito l'utilizzo di dati biometrici per la rilevazione delle presenze dei dipendenti presso un comune vietandone l'ulteriore trattamento. È stato infatti riscontrato, da parte del titolare, il mancato adempimento dell'obbligo di effettuare la notificazione del trattamento e la richiesta di verifica preliminare, non rientrando tale fattispecie nelle ipotesi di esenzione previste dal provvedimento generale in materia di biometria (doc. web n. 4948405)

A seguito di segnalazione di un utente che lamentava la ricezione di *newsletter* promozionali mediante l'utilizzo non autorizzato del proprio indirizzo *e-mail*, siamo intervenuti nei confronti di una società operante nell'*e-commerce* per illecito trattamento di dati per finalità di *marketing* effettuato in base al cd. consenso obbligato dell'interessato raccolto al momento dell'acquisto. Abbiamo quindi vietato l'ulteriore trattamento dei dati per finalità di *marketing* raccolti in assenza di idonea informativa, prescritto le misure necessarie per adeguarsi alla normativa in materia di protezione dati, riservandoci di verificare, con autonomo procedimento, la sussistenza dei presupposti per contestare la violazione amministrativa del caso (doc. web n. 4988238)

In tema di diritto all'oblio, abbiamo dichiarato infondato un ricorso volto ad ot-

tenere la rimozione di alcuni url indicati dal ricorrente e dei relativi *snippet* effettuati a partire dal nome e cognome dell'interessato, protagonista tra la fine degli anni '70 e i primi anni '80 di gravi fatti di cronaca di matrice terroristica. Nonostante il lungo lasso di tempo trascorso dagli eventi abbiamo ritenuto che i fatti narrati riguardino crimini di particolare gravità che vedono il ricorrente come protagonista e rappresentano una delle pagine più buie della storia italiana e debba quindi ritenersi prevalente l'interesse del pubblico (doc. web n. 4988654)

Aprile

A seguito della pubblicazione di fotografie e dati identificativi di una minore associati a precise indicazioni della patologia di cui soffre, siamo intervenuti d'ufficio richiamando l'attenzione delle testate giornalistiche – che nel corso del procedimento hanno spontaneamente rimosso i dati identificativi della minore – alle particolari garanzie poste a tutela dei minori e dei dati idonei a rivelare lo stato di salute. Il diritto del minore alla riservatezza prevale sul diritto di cronaca e neanche il consenso dei genitori autorizza il giornalista a divulgare informazioni che possano nuocere al suo sviluppo (doc. web n 5029484)

Abbiamo risposto ad un quesito in materia di trattamento di dati sanitari posto dal Ministero della salute il quale, unitamente ad Enac, aveva ricevuto la richiesta di una compagnia aerea di inviare al medico competente della società tutta la documentazione sanitaria del personale navigante allo scopo di implementare e perfezionare l'attività di sorveglianza sanitaria, prefigurando tra l'altro la creazione di una banca dati accessibile alla società, al Ministero e all'Aeronautica militare. Il flusso dei dati è stato condizionato ad una adeguata integrazione dei regolamenti sul trattamento dei dati sensibili, che dovranno comunque essere sottoposti al parere vincolante dell'Autorità (doc. web n. 5149198)

Abbiamo condizionato il parere favorevole al Miur sullo schema di decreto concernente il periodo di conservazione di alcune tipologie di dati dell'Anagrafe nazionale degli studenti, richiedendo specifiche garanzie in ordine alla precisazione di un termine entro il quale i dati dovranno essere cancellati o resi anonimi, alle rigorose misure da adottare in ordine al tracciamento e alla conservazione dei *log* relativi agli accessi ed inoltre una limitazione dell'accesso alle sole università (doc. web n. 5029548)

Maggio

Su segnalazione di un cittadino, abbiamo dichiarato illecito e vietato l'ulteriore diffusione di dati sensibili da parte di una regione, che aveva pubblicato e reso accessibili le graduatorie dei partecipanti alle agevolazioni per risparmio energetico, nelle quali erano presenti anche coloro che non risultano destinatari del contributo economico eccedendo quanto previsto dalla normativa sulla trasparenza. La regione ha tempestivamente provveduto alla cancellazione dei dati. Inoltre abbiamo prescritto per il futuro, in assenza di regolamento, di attribuire credenziali di autenticazione ai partecipanti alle procedure selettive ai fini della consultazione relativamente alla collocazione in graduatoria (doc. web n. 5385900)

Abbiamo reso parere ad una regione sullo schema tipo di regolamento delle aziende sanitarie sul trattamento dei dati nei processi di diagnosi e cura elaborato a seguito dell'adozione delle linee guida in tema di *dossier* sanitario, che una volta approvato dalla giunta regionale potrà essere utilizzato dalle aziende sanitarie pubbliche e private operanti nella regione per la stesura del proprio regolamento aziendale. Il predetto schema tiene conto di tutte le prescrizioni già dettate dall'Autorità nell'ambito di uno studio svolto da un importante polo ospedaliero della regione e prevede nell'ambito di ogni processo le soluzioni operative rispettose dei diritti alla cura e alla riservatezza (doc. web n. 5177496)

In tema di propaganda elettorale, siamo intervenuti, a seguito di segnalazione, dichiarando illecito il trattamento di dati effettuati dall'*ex* assessore comunale che aveva utilizzato l'indirizzario istituzionale dell'ente per finalità di propaganda. Le fonti dalle quali sono stati estratti i dati in suo possesso grazie alla carica ricoperta non sono qualificabili come pubblici registri (motivo per cui i dati potrebbero essere estratti a prescindere dal consenso degli interessati) ma rivestono carattere di elenchi ad uso puramente interno. Vietando l'ulteriore trattamento, ci siamo inoltre riservati di verificare con autonomo procedimento la sussistenza dei presupposti per contestare la corrispondente violazione amministrativa (doc. web n. 6358149)

A seguito di verifica preliminare, abbiamo ritenuto lecito il trattamento di dati personali effettuato attraverso la localizzazione di *smarthphone* in dotazione ai dipendenti di una società operanti all'esterno della sede aziendale, al fine di raccogliere i dati necessari per l'elaborazione delle buste paga (pausa pranzo, indennità di viaggio, straordinari). Allo società, che ha stipulato un accordo con le organizzazioni sindacali, sono state prescritte specifiche misure a garanzia dei dipendenti in tema di sicurezza, accesso e conservazione dei dati e il divieto di trattamento di dati ulteriori presenti sul dispositivo (traffico telefonico, *e-mail*) ed inoltre la presenza di un'icona che evidenzi quando la funzionalità è attiva (doc. web n. 5217175)

Abbiamo reso parere favorevole all'intesa tra Agenzia delle entrate e Acquirente unico S.p.A. per la trasmissione dei dati utili all'addebito del canone tv nelle fatture per la fornitura di energia elettrica, prescrivendo per il Sistema di interscambio del flusso dei dati (Sid) l'utilizzo di un collegamento ad avanzata sicurezza per garantire un'efficace protezione oltre che dei dati personali, anche dei sistemi informativi di entrambi gli enti (doc. web n. 5217271)

Giugno

Abbiamo rigettato la richiesta di verifica preliminare e bilanciamento di interessi, presentata da una associazione di imprese nel settore dell'autonoleggio, per la costituzione di una banca dati centralizzata volta a prevenire e contrastare furti e frodi inerenti i veicoli noleggiati, nella quale si intendeva far confluire i dati personali degli intestatari (anche giudiziari) del contratto di autonoleggio (nonché dei conducenti dei veicoli noleggiati) coinvolti a vario titolo in tali fenomeni. Sulla base degli elementi forniti, abbiamo riscontrato un'ingiustificata compressione dei diritti e delle libertà fondamentali dei contraenti/conducenti che, in buona fede, avessero denunciato, anche reiteratamente, eventi illeciti relativi ai veicoli noleggiati (doc. web n. 5306512)

A seguito di una richiesta di verifica preliminare presentata da un istituto di credito operante solo *online*, abbiamo ammesso il trattamento di dati personali e biometrici per l'attivazione di un sofisticato sistema di autenticazione per l'accesso dei clienti alla propria area riservata. Il sistema, gestito da una società esterna (che non avrà accesso ai dati anagrafici dei clienti) e attivabile solo su base volontaria previa manifestazione di uno specifico consenso, genera dopo alcuni accessi un profilo comportamentale originato da vari fattori quali quello della velocità di digitazione e della pressione sullo schermo. Abbiamo ritenuto il trattamento lecito e proporzionato prescrivendo la cancellazione dei dati al termine di ogni accesso (doc. web n. 5252271)

Abbiamo condizionato il parere in ordine ad uno schema di d.lgs. recante modifiche ed integrazioni al Cad ad alcune osservazioni, al fine di rendere maggiormente adeguato il contenuto dello schema di decreto alla disciplina in materia di protezione dati. In particolare, si è evidenziata la necessità di uniformare i termini del testo a quanto previsto dal regolamento europeo in materia di identificazione elettronica e servizi digitali per le transazioni elettroniche nel mercato

interno, di rispettare il principio di pertinenza e non eccedenza dei dati personali in relazione all'inclusione del codice fiscale nel certificato di firma elettronica e di mantenere in capo ai soggetti pubblici l'obbligo di provvedere alla conservazione sicura dei dati (doc. web n. 5177397)

A seguito di numerose segnalazioni riguardanti telefonate a scopo promozionale ricevute da utenti che non avevano prestato il loro consenso, abbiamo avviato, nei confronti dell'operatore telefonico, una attività istruttoria ed ispettiva a seguito della quale abbiamo accertato l'illecito utilizzo dei dati e quindi vietato l'ulteriore trattamento, avviando un autonomo procedimento per contestare le corrispondenti violazioni amministrative (doc. web n. 5436585)

Luglio

A seguito di segnalazioni e reclami da parte dei dipendenti di un Ateneo, abbiamo riscontrato un illecito trattamento di dati personali attraverso i sistemi di comunicazione elettronica vietandone con effetto immediato l'ulteriore utilizzo e disponendo la trasmissione degli atti all'autorità giudiziaria per valutare eventuali illeciti penali. L'università non ha reso la dovuta informativa sulla scorta del presupposto che il MAC *Address* (identificativo *hardware*) non costituisca dato personale (doc. web n. 5407460)

Abbiamo accolto la richiesta di verifica preliminare presentata da Sky inerente un progetto mirato a trasmettere *spot* pubblicitari di diverso contenuto a gruppi differenti di telespettatori sintonizzati sullo stesso programma. Il progetto, destinato solo a coloro che sono in possesso di uno specifico apparecchio di ricezione collegato ad internet, comporta il loro raggruppamento in base a determinate caratteristiche (tipologia di abbonamento, fascia di età, luogo di residenza) ma nel *database* così creato i dati personali saranno anonimizzati e trattati in forma aggregata; dovrà inoltre essere resa una specifica informativa e garantito il diritto di recedere agevolmente in qualsiasi momento dal servizio (doc. web n. 5408313)

Nel rispetto dei princìpi di necessità, proporzionalità, finalità e correttezza abbiamo autorizzato, su istanza del Ministero dell'interno-Questura di Roma, l'utilizzo di un sistema di videosorveglianza per lo stadio Olimpico di Roma (applicabile anche ad altri stadi) che, attraverso la funzione di riconoscimento facciale, fornisca le immagini degli spettatori abbinate automaticamente al nominativo della persona quale risulta dal sistema di controllo degli accessi ai tornelli e dal sistema di biglietteria, da utilizzarsi in caso di condotte delittuose per risalire alla reale identità dell'autore. Abbiamo prescritto che il sistema possa essere utilizzato direttamente ed esclusivamente da operatori appartenenti alle Forze di polizia, che la protezione dei dati sia assicurata con un meccanismo di *strong authentication* e che le società gestori dell'impianto siano designate responsabili del trattamento (doc. web n. 5386852)

Abbiamo reso parere favorevole sullo schema di decreto direttoriale dell'Inps che definisce le specifiche tecniche e le regole di sicurezza per l'acquisizione, la trasmissione e lo scambio di informazioni dei dati contenuti in due delle tre banche dati che costituiscono il casellario dell'assistenza. L'Inps ha accolto, in fase di predisposizione, le indicazioni che abbiamo fornito al fine di garantire un elevato *standard* di sicurezza da seguire nei trattamenti delle informazioni, attraverso specifiche tecniche di anonimizzazione e cifratura (doc. web n. 5385436)

Settembre

Abbiamo reso parere favorevole sullo schema di regolamento recante norme per il funzionamento del registro dialisi e trapianto di una regione, nel quale sono state integralmente recepite le osservazioni che abbiamo formulato, nel corso delle numerose riunioni e contatti informali, volte a garantire un elevato *standard* di tutela dei dati

sensibili. Le indicazioni hanno riguardato, tra l'altro, l'utilizzo di dati aggregati per le finalità di prevenzione e programmazione sanitaria, l'individuazione dei ruoli dei soggetti coinvolti nel trattamento e l'informativa (doc. web n. 5497118)

Al fine di garantire certezza di cura al paziente abbiamo autorizzato l'utilizzo di dati biometrici (impronta digitale) per la rilevazione delle presenze in un'azienda ospedaliera commissariata e sottoposta ad indagine giudiziaria per il diffuso fenomeno di dipendenti infedeli che timbrano al posto di colleghi assenti vista anche l'impossibilità di installare i tornelli dovuta alla struttura dell'ospedale. Il sistema non prevede la creazione di alcun *database* poiché il dato biometrico è residente, sotto forma numerica crittografata, solo nel *badge* ad uso esclusivo del dipendente al quale dovrà essere fornita adeguata informativa (doc. web n. 5505689)

Abbiamo reso parere favorevole sullo schema di convenzione tipo tra AgID ed i soggetti privati fornitori di servizi che decidono di aderire al sistema pubblico di identità digitale (SPID) che va ad integrare la regolamentazione, già oggetto di parere da parte del Garante, in tema di identità digitale. Lo schema di regolamento è stato elaborato tenendo conto delle indicazioni che abbiamo fornito, nel corso di riunioni e contatti, in materia di informativa, utilizzo e conservazione dei dati (doc. web n.5558208)

Ottobre

Abbiamo disposto, in via d'urgenza e nelle more del completamento dell'istruttoria, il blocco temporaneo del trattamento dei dati e dei campioni biologici contenuti in una banca dati genetica a fini di ricerca, ceduta ad una società londinese a seguito di una procedura fallimentare, per assicurare il rispetto della normativa sulla protezione dei dati personali con particolare riferimento alla necessità che gli interessati siano informati della nuova titolarità del trattamento. Anche allo scopo di preservare la sussistenza delle condizioni per la prosecuzione del progetto di ricerca, il provvedimento di blocco ha fatto espressamente salve le sole operazioni funzionali alla conservazione dei campioni biologici e all'individuazione degli interessati per una (eventuale) nuova manifestazione del consenso e per fornire riscontro agli interessati (doc. web n. 5508051)

Abbiamo vietato ad un importante operatore telefonico l'ulteriore trattamento per finalità di *marketing* dei dati personali concernenti le utenze utilizzate nelle campagne promosse per acquisire il consenso della clientela. In particolare, abbiamo dichiarato l'illiceità del trattamento consistente nell'invio di sms di contenuto promozionale, in assenza dello specifico consenso o addirittura a fronte di un espresso diniego all'utilizzo della propria utenza per finalità promozionali da parte degli interessati (doc. web n. 5727908)

Abbiamo autorizzato i trasferimenti di dati personali dal territorio dello Stato italiano verso le imprese presenti negli Stati Uniti che figurano nell'elenco degli aderenti allo "Scudo" tenuto dal Dipartimento del commercio statunitense, in conformità alla decisione di esecuzione (UE) 2016/1250 della Commissione europea del 12 luglio 2016 (doc. web n. 5652873)

Novembre

Abbiamo dichiarato non conforme alla disciplina del Codice, e quindi vietato, il trattamento di dati connesso a una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione, attraverso un algoritmo, di profili reputazionali attraverso la raccolta e verifica di documentazione fornita, su base volontaria, dai soggetti censiti o raccolta in rete. È stata rilevata innanzitutto l'assenza di un'idonea cornice normativa nonché il condizionamento, in base al *rating* attribuito, sulla vita privata e sulla dignità degli individui, elementi cardine della disciplina di protezione dei dati personali. Ulteriori criticità sono state ri-

scontrate nelle misure di sicurezza del sistema, nei tempi di conservazione nonché nell'informativa da rendere agli interessati (doc. web n. 5796783)

Abbiamo accolto la richiesta di verifica preliminare in relazione al trattamento di dati personali da effettuarsi mediante un sistema di videosorveglianza cd. intelligente volto a garantire la sicurezza degli accessi e la tutela del patrimonio della sede istituzionale di una città metropolitana. Il sistema, idoneo a rilevare automaticamente, segnalare e registrare un comportamento o evento anomalo, quale può considerarsi lo scavalco dei tornelli e l'effrazione delle uscite di emergenza, è risultato proporzionato in quanto gli accorgimenti adottati non comportano un pregiudizio dei diritti e delle libertà fondamentali per i possibili interessati (doc. web n. 5796716)

Abbiamo reso parere favorevole ad uno schema di regolamento del Ministero della salute in materia di manifestazione della volontà di accedere alle tecniche di procreazione medicalmente assistita chiedendo alcune modifiche riguardo all'informativa da rendere agli interessati e alla modalità di acquisizione del consenso, nonché alla necessità di informare adeguatamente le coppie che accedono alle tecniche di procreazione medicalmente assistita di tipo eterologo circa la trasmissione dei loro dati, oltre a quelli relativi ai nati, al centro nazionale trapianti, ai fini dell'implementazione dell'apposito Registro nazionale dei donatori di cellule riproduttive (doc. web n. 5763307)

Dicembre

Abbiamo rinnovato le autorizzazioni generali per il trattamento di dati sensibili e giudiziari, per il trattamento dei dati genetici e per il trattamento effettuato per scopi di ricerca scientifica che saranno efficaci fino al 24 maggio 2018, tenuto conto che a decorrere dal 25 maggio 2018 sarà applicabile il regolamento (UE) 2016/679 in materia di protezione dati, salve le modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia e ferme restando le determinazioni eventualmente adottate dall'Autorità in applicazione del citato regolamento

Pur formulando alcune riserve alla luce dei princìpi in materia di protezione dei dati personali, abbiamo espresso, come previsto dalla disciplina sulla trasparenza amministrativa recentemente novellata, l'Intesa con Anac sullo schema delle linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico generalizzato (doc. web n. 5860807)

Abbiamo ritenuto illecito e vietato ad una multinazionale l'ulteriore trattamento effettuato sulle *e-mail* dei dipendenti ed *ex* dipendenti nonché il trattamento effettuato attraverso i dispositivi Blackberry in quanto risultati in contrasto con la normativa sulla *privacy* e con quella lavoristica. Il Garante si è altresì riservato di verificare la sussistenza delle condizioni per l'eventuale applicazione di sanzioni amministrative (doc. web n. 5958296)

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 14

3. I rapporti con il Parlamento e le altre Istituzioni 18

3.1. Le audizioni del Garante in Parlamento 18

3.2. L'Autorità e le attività di sindacato ispettivo e di indirizzo e controllo del Parlamento 19

3.3. L'attività consultiva del Garante sugli atti del Governo 19

3.3.1. I pareri sugli atti regolamentari e amministrativi del Governo 19

3.3.2. I pareri su norme di rango primario 21

3.4. L'esame delle leggi regionali 21

II – L'ATTIVITÀ SVOLTA DAL GARANTE

4. Il Garante e le pubbliche amministrazioni 27

4.1. I trattamenti di dati sensibili e giudiziari presso le pubbliche amministrazioni 27

4.2. Vigilanza sulle grandi banche dati pubbliche 29

4.3. La trasparenza amministrativa 31

4.3.1. L'accesso civico 31

4.3.2. La pubblicazione di dati personali online 32

4.4. La documentazione anagrafica e la materia elettorale 35

4.5. L'istruzione scolastica 37

4.6. L'attività fiscale e tributaria 39

4.7. La videosorveglianza in ambito pubblico 43

4.8. I trattamenti effettuati presso regioni ed enti locali 45

4.9. La previdenza e l'assistenza sociale 49

4.10. L'attività giudiziaria 51

Indice

5. La sanità 54

5.1. I trattamenti per fini di cura 54

5.1.1. L'informativa e il consenso al trattamento dei dati sulla salute 54

5.1.2. Il Fascicolo sanitario elettronico (Fse) 55

5.1.3. I dossier *sanitari* 57

5.1.4. Referti e documentazione sanitaria 58

5.1.5. La tutela della dignità della persona 59

5.1.6. Il trattamento di dati personali in relazione all'accertamento dell'infezione da HIV 60

5.2. I trattamenti di dati sulla salute per fini amministrativi 61

6. I dati genetici 65

7. La ricerca scientifica e la statistica 68

7.1. La ricerca scientifica 68

7.2. La statistica 71

8. I trattamenti da parte di Forze di polizia 73

8.1. Il controllo sul Ced del Dipartimento della pubblica sicurezza 73

8.2. Altri interventi riguardanti le Forze di polizia 73

8.3. Il controllo sul sistema di informazione Schengen 75

9. L'attività giornalistica 76

9.1. I minori 76

9.2. La cronaca giudiziaria 77

9.3. La diffusione delle informazioni *online* 79

10. *Marketing*, profilazione e trattamento dei dati personali 81

10.1. Verifiche preliminari e richieste di autorizzazione 81

10.2. L'attività di controllo dell'Autorità 83

10.3. Telefonate e sms indesiderati a contenuto promozionale 84

10.4. Spam e raccolta di dati personali in internet 86

11. I trattamenti di dati personali effettuati mediante *call center* ubicati al di fuori dell'Unione europea 90

12. Propaganda elettorale 92

Indice

13. Internet e dati personali *online*. Violazioni di dati personali nel settore delle comunicazioni elettroniche 93

14. La protezione dei dati personali nel rapporto di lavoro pubblico e privato 96

14.1. Il trattamento di dati relativi ai dipendenti tramite sistemi di geolocalizzazione 96

14.2. Il trattamento di dati personali dei dipendenti mediante dispositivi e posta elettronica 99

14.3. Pubblicità e trasparenza dei dati dei lavoratori 101

14.4. Il trattamento di dati personali nella gestione del rapporto di lavoro 102

14.5. Il trattamento di dati sulla salute del personale navigante da parte del "medico competente" del vettore aereo 103

15. Le attività economiche 105

15.1. Il settore bancario 105

15.2. Le banche dati interoperatore e i codici di deontologia nel settore economico/finanziario 106

15.3. La videosorveglianza in ambito privato 107

15.4. Il recupero crediti 108

15.5. Attività imprenditoriali e nuove tecnologie 109

16. I dati biometrici 113

16.1. Biometria in ambito pubblico 113

16.2. Il trattamento dei dati biometrici nel rapporto di lavoro 113

17. Attività di normazione tecnica internazionale e nazionale 116

18. Il trattamento dei dati personali nel condominio 117

19. Il trasferimento dei dati all'estero 118

20. Il registro dei trattamenti 121

20.1. La notificazione 121

20.2. L'evoluzione della notificazione nel 2016 121

21. La trattazione dei ricorsi 123

21.1. I profili generali 123

21.2. I dati statistici 124
21.3. La casistica più significativa 125
21.4. I profili procedurali 128

22. Il contenzioso giurisdizionale 129

22.1. Considerazioni generali 129
22.2. I profili procedurali 129
22.3. Le opposizioni ai provvedimenti del Garante 130
22.4. L'intervento del Garante nei giudizi relativi all'applicazione del Codice 136

23. L'attività ispettiva e le sanzioni 137

23.1. La programmazione dell'attività ispettiva 137
23.2. La collaborazione con la Guardia di finanza 138
23.3. I principali settori oggetto di controllo 139
23.4. I provvedimenti adottati dall'Autorità a seguito dell'attività ispettiva 140
23.5. L'attività sanzionatoria del Garante 141
23.5.1. Le violazioni penali e i procedimenti relativi alle misure minime di sicurezza 141
23.5.2. Le sanzioni amministrative 143

24. Le relazioni comunitarie e internazionali 147

24.1. La riforma del quadro giuridico europeo in materia di protezione dei dati 147
24.2. La cooperazione tra autorità di protezione dati nell'UE: il Gruppo Art. 29 147
24.3. La cooperazione delle autorità nel settore libertà, giustizia e affari interni 156
24.4. Le conferenze delle autorità su scala internazionale 158
24.5. La partecipazione ad altri comitati e gruppi di lavoro internazionali 160

25. L'attività di comunicazione, informazione e di rapporto con il pubblico 167

25.1. La comunicazione del Garante: profili generali 167
25.2. I prodotti informativi 168
25.3. I prodotti editoriali e multimediali 168
25.4. Le manifestazioni e le conferenze 171
25.5. Le relazioni con il pubblico 173

26. Studi, documentazione, trasparenza e anticorruzione 176

26.1. Il Servizio studi e documentazione 176

26.2. La biblioteca 177

26.3. L'Autorità trasparente e l'anticorruzione 178

III – L'UFFICIO DEL GARANTE

27. La gestione amministrativa e dei sistemi informatici 183

27.1. Il bilancio e la gestione economico-finanziaria 183

27.2. L'attività contrattuale, la logistica e la manutenzione dell'immobile 185

27.3. L'organizzazione dell'Ufficio 187

27.4. Il personale e i collaboratori esterni 188

27.5. Il settore informatico e tecnologico 189

IV – I DATI STATISTICI 193

Elenco delle abbreviazioni

AgID	Agenzia per l'Italia Digitale
All.	Allegato
Anac	Autorità nazionale anticorruzione
Anpr	Anagrafe nazionale della popolazione residente
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
cap.	capitolo
cd.	cosiddetto/i
cfr.	confronta
CGUE	Corte di giustizia dell'Unione europea
cit.	citato
Codice	Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196)
Corte EDU	Corte europea dei 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
GU	Gazzetta Ufficiale della Repubblica italiana
GUUE	Gazzetta Ufficiale dell'Unione europea
Gruppo Art. 29	Gruppo dei garanti europei istituto dall'art. 29 della direttiva 95/46/CE
l.	legge
lett.	lettera
n.	numero

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

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 2016 l'Autorità ha continuato ad attribuire rilevanza centrale alle iniziative volte a favorire la piena attuazione del nuovo quadro normativo europeo in materia di protezione dei dati personali (cd. pacchetto protezione dati).

Tale impianto, allo stato, è costituito dal regolamento generale sulla protezione dei dati personali – 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 (GUUE 4 maggio 2016, L 119/1) –, pienamente esecutivo a partire dal 25 maggio 2018, e dalla direttiva sulla protezione dei dati nelle attività di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali – 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 (GUUE 4 maggio 2016, L 119/89) –, il cui termine di recepimento nell'ordinamento nazionale è fissato al 6 maggio 2018.

In questo contesto è necessario evidenziare brevemente alcuni elementi legati all'impatto prevedibile che i due strumenti avranno sulla normativa italiana sia primaria, sia secondaria.

In primo luogo, il regolamento generale (UE) 2016/679 sarà integralmente applicabile nell'ordinamento italiano proprio per la sua natura di atto immediatamente esecutivo in ogni sua parte; tuttavia, esso prevede alcuni margini di legiferazione per gli Stati membri dei quali occorre tenere conto. In alcuni casi, infatti, il regolamento impone al legislatore nazionale di emanare disposizioni di "attuazione". Ciò vale, per esempio, rispetto alla definizione dei criteri per l'accreditamento degli organismi incaricati di certificare i trattamenti di dati personali (v. art. 43, par. 1); per l'obbligo di istituire autorità di controllo indipendenti ai sensi dell'art. 51, nonché per l'attribuzione alle stesse delle risorse umane e finanziarie necessarie e per la definizione dei meccanismi di supervisione contabile sulle medesime e dei criteri di nomina dei loro componenti (v. artt. 52 e 53); analogo obbligo di intervento normativo sussiste con riguardo alla definizione delle deroghe alle disposizioni del regolamento necessarie per consentire l'esercizio della libertà di espressione anche giornalistica (v. art. 85,

par. 1 e 2). In altri casi, invece, il regolamento consente al legislatore nazionale di intervenire, ove lo si ritenga necessario, per "mantenere o introdurre disposizioni più specifiche" tese ad "adeguare l'applicazione delle norme" del regolamento ai trattamenti svolti nel pubblico interesse, ovvero, in ottemperanza a obblighi di legge (art. 6, par. 2) e per "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute" (art. 9, par. 4). Tale margine di intervento si concretizza, in altri casi ancora, attraverso l'indicazione di una serie di opzioni nel cui ambito il legislatore nazionale sarà chiamato a operare una scelta: si veda, in particolare, la definizione della soglia di età per la validità del consenso prestato dal minore (art. 8, par. 1), la possibilità di prevedere meccanismi di autorizzazione preventiva da parte dell'autorità per alcuni trattamenti svolti nel pubblico interesse (art. 36, par. 5), come anche casi ulteriori di nomina obbligatoria di un Responsabile della protezione dei dati (DPO) di cui all'art. 37, par. 4, ovvero disposizioni più specifiche per disciplinare il trattamento dei dati personali nel rapporto di lavoro "con legge o contratti collettivi" ai sensi dell'art. 88. Resta ferma, infine, la possibilità di introdurre nel diritto nazionale specifiche deroghe a singole disposizioni del regolamento, seppure nel rispetto delle condizioni indicate nella norma di riferimento: si vedano, in particolare, i casi menzionati all'art. 23 e all'art. 89, par. 2 e 3, del regolamento.

In tutti questi casi il regolamento prevede come termine per l'adozione delle misure normative di attuazione il 25 maggio 2018, coerentemente con l'impianto della riforma che mira a garantire l'applicazione uniforme della normativa in materia a partire da tale data nell'intera Unione europea. Occorre precisare che, quando il regolamento fa riferimento a una base giuridica o a una misura legislativa, "ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato" (considerando 41 del regolamento); laddove consentito dal quadro costituzionale, appare, quindi, possibile demandare l'adozione di misure ad autorità diverse dal Parlamento.

Per quanto concerne la direttiva (UE) 2016/680, bisogna evidenziare come essa abbia natura di *lex specialis* rispetto al regolamento generale sulla protezione dei dati, di cui declina princìpi e obblighi con riguardo allo specifico contesto di attività e ai poteri delle autorità di polizia e giudiziarie. Di tale caratteristica non si potrà non tenere conto nell'*iter* nazionale di recepimento, garantendo i necessari raccordi con il regolamento e intervenendo sulle norme già vigenti in un'ottica di semplificazione e armonizzazione (si vedano, soprattutto, gli artt. 53-57 del Codice). A tale riguardo va segnalato che il disegno di legge che delega il Governo al recepimento delle direttive europee e all'attuazione di altri atti dell'Unione europea ("Legge di delegazione europea 2016") è stato poi approvato, in via definitiva, dal Consiglio dei ministri il 28 aprile 2017 e prevede specificamente la delega per l'attuazione della citata direttiva (UE) 2016/680.

Risulta evidente, pertanto, che l'impatto del pacchetto protezione dati sul quadro normativo vigente si configura come complesso e pluristratificato, in termini di normazione primaria (Codice in materia di protezione dei dati personali) e secondaria (regolamenti attuativi del Codice, anche ministeriali, e altre disposizioni adottate dal Garante nel corso degli anni, comprese autorizzazioni generali, codici deontologici, provvedimenti generali). Non si può non ricordare, in proposito, come la giurisprudenza della Corte di giustizia dell'Unione europea abbia ampiamente delineato quali debbano essere i criteri che presiedono agli interventi normativi nazionali (da intendersi *lato sensu*, con riguardo alla loro natura di atti anche non parlamentari) in presenza di una norma regolamentare europea, consentendo tali interventi solo entro limiti precisi e stringenti.

Per parte sua, l'Autorità ha iniziato un'ampia e approfondita analisi, diretta a evidenziare le azioni esperibili sin da subito nell'ambito dei poteri che le sono conferiti dall'attuale ordinamento. In questo senso, partecipa attivamente ai lavori che il Gruppo Art. 29 sta conducendo fin dai primi mesi del 2016 per sviluppare una serie di strumenti interpretativi e applicativi del regolamento e della direttiva – che sono diffusamente illustrati al par. 24.2 cui si fa rinvio – ed ha promosso la conoscenza fra il pubblico di alcuni istituti innovativi quali il "responsabile della protezione dei dati", il diritto alla portabilità dei dati e il nuovo meccanismo di decisione fra le autorità competenti nell'UE (cd. sportello unico). Il Gruppo Art. 29 ha, fra l'altro, elaborato alcune linee guida applicative del regolamento (sui responsabili della protezione dei dati, sulla designazione dell'autorità capofila e in materia di diritto alla portabilità) che intendono indicare ai titolari di trattamento pubblici e privati alcune azioni che possono essere intraprese sin d'ora in quanto si fondano su disposizioni precise del regolamento, che non lasciano all'intervento del legislatore nazionale quegli spazi a cui si è innanzi fatto cenno. I tre documenti sono stati pubblicati sul sito istituzionale del Gruppo Art. 29 il 13 dicembre 2016 e sono stati aperti alla consultazione pubblica fino al 15 febbraio 2017 (par. 24.2).

Queste attività proseguiranno nel corso del 2017 e si intensificheranno anche attraverso il coinvolgimento dell'Autorità come *partner* in progetti internazionali, finanziati dalla Commissione europea, tesi a potenziare le capacità amministrative e gestionali delle autorità di protezione dati in vista degli appuntamenti del maggio 2018.

1.2. Di particolare rilievo è stata l'attività dell'Autorità diretta a collaborare con il Governo e le altre pubbliche Amministrazioni mediante il rilascio di pareri su schemi di decreti legislativi (par. 2.1.2).

Si segnalano, fra questi, il parere del 3 marzo 2016 (n. 92, doc. web n. 4772830), reso nel corso dei lavori parlamentari che hanno portato all'adozione del decreto legislativo 25 maggio 2016, n. 97, recante revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza (che modifica la l. 6 novembre 2012, n. 190, in materia di prevenzione e repressione della corruzione e dell'illegalità nella pubblica amministrazione ed il d.lgs. 14 marzo 2013, n. 33, finalizzato a rafforzare la trasparenza amministrativa).

Il Garante è, inoltre, intervenuto, con parere del 9 giugno 2016 (n. 255, doc. web n. 5177397), nella fase di approvazione del decreto legislativo 26 agosto 2016, n. 179, che apporta modifiche ed integrazioni al codice dell'amministrazione digitale (Cad), di cui al d.lgs. 7 marzo 2005, n. 82.

Elevato è stato l'impegno diretto a rendere pareri su schemi di atti regolamentari ed amministrativi suscettibili di incidere sulla protezione dei dati personali (par. 3.3.1), che hanno spesso riguardato materie di notevole rilevanza giuridica e sociale. Molti di questi pareri hanno avuto ad oggetto interventi normativi o atti attuativi volti a dare ulteriore impulso, in diversi ambiti, al processo di digitalizzazione della pubblica amministrazione, come la disciplina in materia: di modalità di assegnazione e utilizzo della Carta elettronica per l'aggiornamento e la formazione del docente di ruolo; di adesione al sistema pubblico per la gestione dell'identità digitale (Spid) per i privati fornitori di servizi (schema di convenzione della Presidenza del Consiglio dei ministri e dell'AgID; sempre in materia di Spid è stato reso il parere sulla convenzione fra l'AgID ed i gestori di identità digitale, da adottare ai sensi dell'art.10, comma 2, d.P.C.M. 24 ottobre 2014); di trasmissione telematica dei dati delle spese sanitarie sostenute presso strutture autorizzate e non accreditate per l'erogazione dei servizi sanitari; di trasmissione telematica all'Agenzia delle entrate e di utilizzo di dati relativi a spese sanitarie e a spese veterinarie; di criteri e modalità di

attribuzione e utilizzo della carta elettronica *ex* art.1, comma 979, l. 28 dicembre 2015, n. 208 e successive modificazioni; di specifiche modalità di realizzazione di una banca dati di beni culturali illecitamente sottratti; di istituzione, con decreto del Ministro dell'interno di concerto con il Ministro della giustizia, della banca dati del dna. Fra le altre materie oggetto di pareri del Garante si segnalano quelle della manifestazione della volontà di accedere alle tecniche di procreazione medicalmente assistita, in attuazione dell'art. 6, comma 3, della l. 19 febbraio 2004, n. 40; della tenuta e aggiornamento degli albi, degli elenchi e dei registri da parte dei Consigli dell'ordine degli avvocati; della determinazione dell'età dei minori non accompagnati vittime di reato; della *compliance* fiscale internazionale e normativa FATCA (*Foreign Account Tax Compliance Act*); dell'Anagrafe nazionale studenti (Ans) con riguardo al trattamento dei dati relativi ai percorsi scolastici, formativi e in apprendistato dei singoli studenti e loro valutazione; dei flussi di dati che possono essere trasmessi al Ministero della salute e alle regioni in relazione alla tessera sanitaria; delle modalità di accesso alle spese sanitarie.

La posizione del Garante è stata, inoltre, rappresentata nell'ambito di numerose audizioni, sia formali che informali, rese presso le competenti Commissioni parlamentari (par. 3.1). La collaborazione istituzionale con il Governo si è, poi, realizzata fornendo, nella materia della protezione dei dati personali, elementi valutativi utili ai fini della risposta su nove atti di sindacato ispettivo e attività di indirizzo e controllo del Parlamento (par. 3.2) ed esprimendo le proprie osservazioni in relazione a undici leggi regionali sottoposte al vaglio di costituzionalità del Governo ai sensi dell'art. 127 della Costituzione (par. 3.4).

1.3. La raccolta indiscriminata e massiva di dati personali da parte di agenzie governative e colossi del web, anche in funzione di contrasto del terrorismo e della criminalità informatica, pone il problema dell'impatto che strumenti di controllo sempre più invasivi hanno non solo sull'economia e sull'organizzazione sociale, ma anche sulla vita privata e sullo stesso sistema democratico. Questi temi hanno costituito l'oggetto del Convegno "La società sorvegliata. I nuovi confini della libertà" organizzato dal Garante in occasione della X Giornata europea della protezione dei dati personali tenutasi il 28 gennaio 2016.

In questo contesto si è confermata l'attenzione dell'Autorità per le grandi banche dati pubbliche, che hanno costituito oggetto di interventi di vigilanza sia in via generale (par. 4.2) sia con particolare riguardo ai trattamenti da parte di Forze di polizia (cap. 8); in quest'ultimo settore il Ministero dell'interno ha richiesto il parere del Garante su due schemi di decreto, da adottarsi ai sensi degli artt. 53 e 57 del Codice, in materia di trattamenti non occasionali effettuati con strumenti elettronici per finalità di polizia e di modalità di attuazione dei princìpi del Codice relativamente al trattamento dei dati effettuato sempre per tali finalità. Il Ministero dell'interno ha, inoltre, comunicato, con riferimento all'anno 2016, di aver posto in essere le misure che ancora al 2015 non risultavano attuate, tra quelle prescritte dal Garante per rafforzare la sicurezza nel trattamento dei dati effettuati per l'attuazione della Convenzione di Schengen (provv. 12 novembre 2009, doc. web n. 2330104).

È, parimenti, proseguita l'azione di vigilanza sui trattamenti effettuati nell'ambito della rete (cap. 13).

In particolare, quanto all'attuazione delle prescrizioni impartite a Google Inc. con il provvedimento del 10 luglio 2014, n. 353 (doc. web n. 3283078), l'Autorità, in conformità a quanto previsto da un apposito protocollo di verifica, ha ricevuto nel corso del 2016 aggiornamenti trimestrali circa l'implementazione di una serie di

misure a tutela degli utenti dei circa 70 servizi offerti, volte a fornire ai medesimi informazioni più numerose e di più agevole reperibilità sul trattamento dei loro dati. Google ha altresì implementato le misure per acquisire il consenso all'uso dei dati non solo per gli utenti autenticati, ma anche – sulla base di una specifica prescrizione del Garante – di quelli non autenticati. Sono state incrementate le possibilità di scelta e le opzioni a disposizione degli utenti in diversi ambiti (annunci pubblicitari; raccolta dei dati per la cronologia delle ricerche e delle localizzazioni o per l'attività vocale e audio; opposizione al trattamento dei dati esercitabile anche solo rispetto ad alcuni servizi e incroci di dati tra servizi diversi). Come prescritto dal Garante, Google rende inaccessibili i dati dell'utente autenticato 24 ore dopo la richiesta dell'interessato e li cancella entro 2 mesi, se i dati risiedono su sistemi attivi, o entro 6 mesi, se sono archiviati su sistemi di *back up*. I cd. dati di sistema, necessari a Google per fornire i propri servizi (es. i *file* di *log*), vengono invece anonimizzati allo scadere di tempi di conservazione predefiniti.

Di particolare rilievo è stata la reazione dell'Autorità all'iniziativa del 25 agosto 2016 con cui WhatsApp Inc. – società del gruppo Facebook Inc. – ha modificato le regole contenute nei "termini e informativa sulla *privacy*" in relazione ai propri servizi di messaggistica rendendo pubblici, tramite il proprio *blog* https://blog.whatsapp.com, i termini essenziali dell'operazione con l'effetto, in sostanza, di mettere a disposizione di Facebook le informazioni concernenti i singoli *account* WhatsApp. Il Garante – d'intesa con altre autorità europee di protezione dei dati – ha richiesto informazioni alle società coinvolte al fine di verificare la complessiva correttezza dei trattamenti effettuati e sta valutando i riscontri forniti.

1.4. In ambito sanitario, l'Autorità, oltre ad intervenire per contrastare diverse tipologie di violazioni dei diritti dei pazienti, ha fornito numerosi chiarimenti sia ai singoli cittadini, che alle Istituzioni operanti in materia.

Particolare menzione meritano la partecipazione al tavolo di lavoro del Cantiere sanità digitale, organizzato dal Forum PA, con il contributo scientifico dell'Osservatorio innovazione digitale in sanità del Politecnico di Milano, nonché la corrispondenza intercorsa tra il Presidente dell'Autorità e il Presidente della Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri (nota 17 maggio 2016), nell'ambito della quale l'Autorità ha fornito chiarimenti su varie questioni relative al trattamento dei dati dei pazienti (modalità di raccolta del consenso dell'interessato; presupposti legittimanti i trattamenti per fini amministrativi effettuati dai medici; misure di sicurezza da adottare per il trattamento dei dati personali con strumenti informatici; formazione del personale coinvolto nel processo di cura dell'interessato; garanzie per il trasferimento dei dati all'estero).

Inoltre anche nel 2016 l'Autorità ha preso parte ai lavori del tavolo tecnico di monitoraggio e indirizzo per l'attuazione delle disposizioni inerenti il Fascicolo sanitario elettronico (Fse), cui partecipano anche il Ministero dell'economia e delle finanze, l'AgID, il Cnr, il coordinamento regionale e i rappresentanti di numerose regioni, sotto la direzione del Ministero della salute. La disciplina in materia di Fse è stata, peraltro, innovata da un emendamento di modifica dell'art. 12, d.l. 18 ottobre 2012, n. 179, convertito in l. 17 dicembre 2012, n. 221 (art. 1, comma 382, legge di bilancio 2017).

1.5. Con riferimento ai trasferimenti di dati personali all'estero va segnalata per la sua importanza l'autorizzazione 27 ottobre 2016, n. 436 (doc. web n. 5652873), con cui il Garante si è conformato – ai sensi dell'art. 44, comma 1, lett. *b*), del Codice – alla decisione di esecuzione (UE) 2016/1250 della Commissione europea

del 12 luglio 2016 (in GUUE 1° agosto 2016, n. L 207) e ha autorizzato, per quanto di competenza nazionale, i trasferimenti di dati personali dall'Unione europea ad organizzazioni aventi sede negli Stati Uniti d'America (cap. 19).

La decisione della Commissione ha fatto seguito alla sentenza della CGUE 6 ottobre 2015 (causa C-362/14, Maximillian Schrems v. Data Protection Commissioner, su cui v. Relazione 2015, p. 161), che aveva invalidato la decisione 2000/250/CE relativa al precedente accordo detto *Safe Harbor* (cd. regime di Approdo sicuro) e ha riconosciuto che il nuovo Accordo denominato "EU-U.S. *Privacy Shield*" (cd. Scudo UE-USA per la *privacy*), basato sui princìpi emanati dal Dipartimento del commercio degli Stati Uniti il 7 luglio 2016, garantisce un livello adeguato di protezione dei dati personali oggetto dei suddetti trasferimenti.

1.6. In materia di protezione dei dati personali nell'ambito del rapporto di lavoro pubblico e privato – a seguito del completamento nel 2015 della cd. riforma del lavoro (o *Jobs Act*) con i decreti legislativi di attuazione della legge-delega n. 183/2014 – specifica menzione meritano gli interventi del Garante in relazione alla nuova disciplina dei controlli a distanza dell'attività dei lavoratori, innovata dall'art. 23, d.lgs. n. 151/2015, che ha modificato l'art. 4, l. n. 300/1970, recante lo Statuto dei lavoratori.

In particolare, un provvedimento del Garante ha rappresentato la prima occasione in cui l'Autorità ha espresso il proprio orientamento sull'ambito di applicazione del comma 2 del predetto art. 4 dello Statuto dei lavoratori, come ora modificato, 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) (par. 14.2).

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 2016 sono stati approvati numerosi provvedimenti normativi che hanno riflessi sulla disciplina riguardante la protezione dei dati personali. Fra questi, al fine di offrirne una ricognizione, seppur sintetica, tale però 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 2017

1) la legge 11 dicembre 2016, n. 232 recante Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019. Il comma 243 di suddetta legge, nel modificare l'art. 24-*bis*, d.l. 22 giugno 2012, n. 83, convertito, con modificazioni, dalla l. 7 agosto 2012, n. 134, stabilisce le misure da applicare alle attività svolte da *call center* indipendentemente dal numero di dipendenti occupati. Le nuove regole per il funzionamento dei *call center* prevedono in particolare che, quando un utente effettua o riceve una chiamata dagli stessi, deve essere informato preliminarmente riguardo al Paese in cui è fisicamente collocato l'operatore che risponde; l'operatore del *call center* collocato in un Paese *extra*-UE deve, inoltre, offrire subito la possibilità di richiedere che il servizio sia reso da un operatore collocato nel territorio nazionale o nella UE, con immediato trasferimento nel corso della medesima chiamata. Diviene obbligatorio per tutti gli operatori economici che svolgono attività di *call center*, iscriversi al registro degli operatori di comunicazione tenuto dall'Autorità per le garanzie nelle comunicazioni, alla quale dovranno essere fornite tutte le numerazioni telefoniche messe a disposizione del pubblico e utilizzate per i servizi di *call center*. Per chi decide di localizzare, anche mediante affidamento a terzi, l'attività di *call center* in un Paese *extra*-UE, diventa obbligatorio darne comunicazione almeno trenta giorni prima del trasferimento alle seguenti amministrazioni: Ministero del lavoro e delle politiche sociali nonché Ispettorato nazionale del lavoro; Ministero dello sviluppo economico e Garante per la protezione dei dati personali.

Una particolare novità, introdotta dalla legge di bilancio 2017, è quella della responsabilità solidale tra committente e gestore del *call center*: chi affida il servizio ad un *call center* esterno è responsabile in solido con il soggetto gestore. Merita attenzione, inoltre, il comma 608 secondo il quale, 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 - *passenger name record*) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e nelle more del suo recepimento, è autorizzata la spesa di 5,5 milioni di euro per l'anno 2017 e di 16 milioni di euro per l'anno 2018 per la realizzazione della piattaforma informatica necessaria e di 4,5 milioni di euro a decorrere dall'anno 2019 per la gestione e la manutenzione della stessa;

***Screening* neonatali**

2) la legge 19 agosto 2016, n. 167, introduce nel nostro ordinamento Disposizioni in materia di accertamenti diagnostici neonatali obbligatori per la prevenzione e la cura delle malattie metaboliche ereditarie. La legge ha la finalità di garantire la

prevenzione delle malattie metaboliche ereditarie, attraverso l'inserimento nei livelli essenziali di assistenza (LEA) degli *screening* neonatali obbligatori, da effettuare su tutti i nati a seguito di parti effettuati in strutture ospedaliere o a domicilio, per consentire diagnosi precoci e un tempestivo trattamento delle patologie. In particolare, l'art. 3 prevede l'istituzione, presso l'Istituto superiore di sanità, del Centro di coordinamento sugli *screening* neonatali al quale vengono affidati, tra gli altri, per quanto di interesse dell'Autorità, i compiti di seguito riportati: a) fornire informazioni codificate e standardizzate ai servizi territoriali per l'assistenza alle famiglie dei neonati sui rischi derivanti dalle patologie metaboliche ereditarie, nonché sui benefici conseguibili attraverso l'attività di *screening*, offrendo anche informazioni sulla terapia e sulle migliori cure disponibili per la specifica malattia metabolica; b) stabilire le modalità di raccolta dei campioni di sangue nonché di consegna dei medesimi, entro quarantotto ore dal prelievo, presso i centri di *screening* di riferimento per la regione; c) istituire un archivio centralizzato sugli esiti degli *screening* neonatali al fine di rendere disponibili dati per una verifica dell'efficacia, anche in termini di costo, dei percorsi intrapresi. Con riferimento all'archivio centralizzato (art. 3, comma 4, lett. *g*), si segnala l'accoglimento di un ordine del giorno di particolare interesse per l'Autorità (9/3504-A/2, a firma degli on.li Fontana e Palese), il quale, in considerazione dell'importanza dei dati in esso contenuti che "oltre ad essere preziosi per la lotta ad alcune gravi patologie, costituiscono, in ogni caso dati altamente sensibili, il cui uso improprio o abusivo può essere fonte di violazione del diritto alla *privacy*, disciplinata dal Codice in materia di protezione dei dati personali", impegna il Governo "a valutare l'opportunità di rivolgersi al Garante per la protezione dei dati personali, ai sensi del comma 4 dell'art. 154 del d.lgs**.** 30 giugno 2003, n. 196, al fine di acquisire ogni utile elemento per fare quanto di propria competenza perché sia garantita la protezione dei dati personali trattati nell'ambito dell'attuazione del disegno di legge (…)".

Il Garante in passato (cfr. Relazione 2015, p. 79) aveva espresso un parere su uno schema di decreto concernente lo *screening* neonatale esteso (SNE) ai fini della diagnosi precoce di patologie metaboliche ereditarie e in tale occasione (v. doc. web n. 3943315), considerata la delicatezza dei flussi informativi, aveva richiamato l'attenzione di tutti i soggetti coinvolti sull'esigenza di assicurare le garanzie previste in materia di protezione dei dati personali. Le condizioni poste dal Garante in suddetto parere sono state recepite dal Ministero della salute nel decreto del 13 ottobre 2016, recante Disposizioni per l'avvio dello *screening* neonatale per la diagnosi precoce di malattie metaboliche ereditarie. La legge 19 agosto 2016, n. 167, al riguardo, fa un ulteriore passo avanti in quanto prevede l'inserimento dello SNE nei nuovi livelli essenziali di assistenza così da poterlo garantire a tutti i nuovi nati.

Contrasto a terrorismo

3) la legge 28 luglio 2016, n. 153, reca le Norme per il contrasto al terrorismo, nonché per la ratifica ed esecuzione: a) della Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, adottata a Varsavia il 16 maggio 2005; b) della Convenzione internazionale per la soppressione di atti di terrorismo nucleare, adottata a New York il 14 settembre 2005; c) del Protocollo di emendamento alla Convenzione europea per la repressione del terrorismo, adottato a Strasburgo il 15 maggio 2003; d) della Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo, adottata a Varsavia il 16 maggio 2005; e) del Protocollo addizionale alla Convenzione del Consiglio d'Europa per la prevenzione del terrorismo, adottato a Riga il 22 ottobre 2015. La legge in parola introduce modifiche al codice penale, prevedendo nuove fattispecie di reato tra cui il finanziamento di condotte con fina-

lità di terrorismo ed individua all'art. 9, l'UIF (Unità di informazione finanziaria), istituita dal d.lgs. n. 231/2007, come autorità di *intelligence* finanziaria, ai sensi della Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato;

4) la legge 28 luglio 2016, n. 155 recante Ratifica ed esecuzione dell'Accordo sulla cooperazione di polizia e doganale tra il Governo della Repubblica italiana e il Consiglio federale svizzero, adottato a Roma il 14 ottobre 2013, sancisce l'impegno dei due Paesi a rafforzare la cooperazione transfrontaliera, anche sul versante degli scambi di informazioni e di esperienze, con la finalità di contrastare efficacemente la criminalità nelle sue varie forme e le attività di carattere terroristico. Si tratta di una cooperazione ampia che si richiama ad analoghe forme definite all'interno dell'Unione europea, prima con il cd. Trattato di Prüm del 27 maggio 2005 e quindi con le decisioni 2008/615/GAI e 2008/616/GAI. La Svizzera è parte della Cooperazione Schengen pur non appartenendo all'Unione europea. Per quanto di interesse si segnala che l'attuazione concreta della collaborazione avverrà mediante scambi di informazioni a livello bilaterale, nonché di esperienze maturate dagli organi competenti delle due Parti. Vi saranno, inoltre, moduli formativi congiunti soprattutto per i servizi da assicurare nelle zone frontaliere, nonché l'utilizzo di tecniche specialistiche per contrastare le varie forme di criminalità. Per quanto riguarda l'adozione di misure congiunte, queste riguarderanno la sorveglianza della frontiera comune, servendosi eventualmente di unità miste, e il contrasto ai traffici illeciti di stupefacenti mediante consegne controllate transfrontaliere (per quest'ultimo profilo, secondo le linee guida già contenute nell'intesa esecutiva italo-svizzera del 17 novembre 2009). In ogni caso, la cooperazione prevista dall'Accordo in esame avrà luogo sulla base di richieste di assistenza della Parte interessata: una richiesta potrà anche essere rigettata, se si ritenga che dall'esecuzione di essa possano essere compromessi la sovranità, la sicurezza, l'ordine pubblico o altri interessi fondamentali della Parte adita. È anche previsto che in casi particolari le autorità competenti possano spontaneamente comunicarsi informazioni utili a prevenire minacce concrete alla sicurezza, all'ordine pubblico e al contrasto alla criminalità (cfr. Titolo II, artt. 5-10). È altresì previsto che le Parti cooperino in base alle rispettive normative nazionali per la protezione dei testimoni e dei loro familiari, soprattutto mediante lo scambio delle necessarie informazioni. Qualora sussista un pericolo grave ed imminente per la vita o l'integrità fisica delle persone, gli agenti di una Parte potranno attraversare la frontiera comune senza la preventiva autorizzazione dell'altra Parte contraente, per adottare le più opportune misure. Gli agenti che intervengono in questo ambito sono comunque tenuti a rispettare la normativa nazionale della Parte sul cui territorio operano, e successivamente a informare con sollecitudine le competenti autorità. È anche previsto che in caso di eventi catastrofici dovuti alla natura o all'attività dell'uomo o di sinistri gravi, salvaguardando le disposizioni della Convenzione italo-elvetica del 1995 in materia, le autorità competenti si assistano reciprocamente con lo scambio di informazioni e il coordinamento delle misure da adottare (cfr. Titolo III, artt. 11-22). Strettamente correlati e di interesse per l'Autorità appaiono il Titolo V (artt. 27 e 28) e il Titolo VI (artt. 29 e 30), rispettivamente concernenti l'organizzazione e il funzionamento del centro comune di cooperazione di polizia e doganale italo-elvetico, con particolare riguardo alla gestione delle informazioni e alla protezione dei dati scambiati nell'ambito della cooperazione bilaterale. È previsto in particolare che le autorità competenti dei due Paesi si impegnino a garantire un livello di protezione dei dati personali conforme a quanto previsto in materia dalla Convenzione del Consiglio d'Europa del 28 gennaio 1981. I dati personali sensibili, in particolare, dovranno essere utilizzati solo

per gli scopi previsti dall'Accordo, ottemperando alle condizioni poste dalla Parte che li ha trasmessi. Le informazioni e i documenti trasmessi in base all'Accordo in esame non potranno essere divulgati a terzi né utilizzati per finalità diverse da quelle stabilite dall'Accordo, se non previa approvazione scritta dell'autorità competente che li ha forniti. In sede di approvazione del testo il Governo ha accolto un ordine del giorno (9/3767/1, a firma dell'on. Michela Marzano), con cui si è impegnato a valutare l'opportunità di rivolgersi al Garante nella fase attuativa dell'Accordo per gli aspetti che attengono alla tutela dei dati personali;

Ratifica ed esecuzione della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea

5) la legge 21 luglio 2016, n. 149 recante 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, e delega al Governo per la sua attuazione. Delega al Governo per la riforma del libro XI del codice di procedura penale. Modifiche alle disposizioni in materia di estradizione per l'estero: termine per la consegna e durata massima delle misure coercitive. A tal fine il Governo è delegato ad introdurre entro sei mesi dall'entrata in vigore della legge, uno o più decreti legislativi secondo i princìpi e criteri direttivi individuati e che, per quanto di interesse, attengono alla:

a) previsione di norme volte a migliorare la cooperazione giudiziaria in materia penale da parte dell'Italia verso gli Stati parte della Convenzione, senza pregiudizio di quelle poste a tutela della libertà individuale;
b) modifica e integrazione delle disposizioni dell'ordinamento al fine di assicurare che l'assistenza giudiziaria dell'Italia verso gli Stati parte della Convenzione sia attuata in maniera rapida ed efficace, fermo restando il rispetto dei diritti individuali e dei princìpi della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, adottata a Roma il 4 novembre 1950 e resa esecutiva dalla l. 4 agosto 1955, n. 848;
c) disciplina delle richieste, delle informazioni e delle operazioni di intercettazione delle telecomunicazioni all'estero, conformemente a quanto stabilito dal Titolo III della Convenzione e nel rispetto dei princìpi fondamentali dell'ordinamento giuridico dello Stato.

L'art. 5 della legge introduce particolari modifiche alle disposizioni del codice di procedura penale in tema di estradizione per l'estero a tutela dei diritti fondamentali, stabilendo i termini per la consegna e la durata massima delle misure coercitive.

In sede di approvazione del testo anche, in questo caso, il Governo ha accolto un ordine del giorno (9/3944/2, a firma dell'on. Michela Marzano) impegnandosi a valutare l'opportunità di rivolgersi al Garante in fase attuativa della delega per gli aspetti che attengono alla tutela dei dati personali.

Legge di delegazione europea

6) la 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).

Fra gli atti ai quali il Governo è chiamato a dare attuazione rilevano, per gli aspetti di protezione dei dati personali:

a) la direttiva (UE) 2015/565 della Commissione dell'8 aprile 2015, che modifica la direttiva 2006/86/CE e disciplina alcune prescrizioni tecniche in materia di tessuti e cellule umani, attinenti, tra l'altro, alla codifica, alla lavorazione, alla conservazione, allo stoccaggio ed alla distribuzione degli stessi. Tali prescrizioni devono assolvere alla funzione di rendere rintracciabili i tessuti e le cellule prelevati, lavorati, stoccati o distribuiti sul territorio degli Stati membri, nel percorso dal donatore al ricevente e viceversa (direttiva 2004/23/CE, art. 8). In base alle modifiche di cui alla direttiva (UE) 2015/565, la rintracciabilità dei tessuti e delle cellule avrà luogo (art. 9,

direttiva 2006/86/CE) in particolare grazie alla documentazione e all'uso del codice unico europeo. Tale codice, funzionale a garantire l'uniformità dei sistemi di identificazione già adoperati nei singoli Stati membri ai sensi della direttiva 2006/86/CE, dovrà essere impiegato per tutti i tessuti e le cellule distribuiti nell'Unione europea a fini di applicazioni sull'uomo (in base al testo dell'art. 10 della direttiva 2006/86/CE e fatte salve le eccezioni ivi contemplate). La direttiva, inoltre, stabilisce le prescrizioni minime che gli istituti dei tessuti, compresi quelli importatori, dovranno osservare, con riferimento all'applicazione del codice unico europeo. Tra esse, si ricordano: l'assegnazione del codice ai tessuti e cellule prima della distribuzione; l'assegnazione di una sequenza di identificazione della donazione dopo l'approvvigionamento dei tessuti e delle cellule o al momento del loro ricevimento da un'organizzazione di approvvigionamento o all'atto dell'importazione da un fornitore di un Paese terzo; l'applicazione del codice sull'etichetta in modo indelebile e permanente. La direttiva prescrive, altresì, che le autorità competenti degli Stati membri assicurino: l'individuazione delle strutture operanti, mediante l'assegnazione di un numero unico per ogni istituto dei tessuti (accreditato, designato, autorizzato o titolare di licenza); l'assegnazione di numeri unici della donazione; la piena applicazione del codice unico europeo ed il relativo monitoraggio; la convalida e l'aggiornamento dei dati (per il proprio Stato membro) sugli istituti dei tessuti contenuti nel compendio degli istituti dei tessuti dell'UE. Prevede anche la predisposizione di una piattaforma informatica (piattaforma di codifica dell'UE), gestita dalla Commissione europea e disponibile al pubblico prima del 29 ottobre 2016. Tale piattaforma contiene il compendio degli istituti dei tessuti dell'UE ed il compendio dei prodotti di tessuti e cellule dell'UE. In attuazione della predetta direttiva il Governo ha emanato il d.lgs. 16 dicembre 2016, n. 256 recante prescrizioni tecniche relative alla codifica di tessuti e cellule umani;

b) la direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che introduce innovative previsioni sulla trasparenza e sull'accesso a informazioni relative alla titolarità effettiva di società e *trust* e richiama l'applicazione delle regole in tema di trattamento dei dati personali, regolandone i rapporti con le esigenze dell'antiriciclaggio. L'art. 15 della l. n. 170/2016, contiene i princìpi e criteri direttivi cui deve attenersi il Governo delegato ad adottare le necessarie disposizioni attuative e prevede espressamente che le stesse siano adottate previo parere del Garante;

Legge europea 2015-2016

7) la legge 7 luglio 2016, n. 122 reca le Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea (legge europea 2015-2016). L'art. 36 prevede, per lo svolgimento dei compiti connessi all'attuazione della disciplina europea, un meccanismo stabile di finanziamento pubblico per il Garante, ancorché limitato nel suo ammontare, anche in ragione delle competenze allo stesso attribuite nell'ambito del nuovo quadro legislativo europeo in materia di protezione dei dati personali. La disposizione, infatti, stabilisce che "al fine di assicurare il funzionamento del Garante per la protezione dei dati personali e il regolare svolgimento dei poteri di controllo ad esso affidati dalla normativa dell'Unione europea, il fondo di cui all'articolo 156, comma 10, del codice di cui al decreto legislativo 30 giugno 2003, n. 196, è incrementato nella misura di 12

milioni di euro annui a decorrere dall'anno 2017". L'art. 7 della citata legge disciplina infine l'accesso e l'utilizzo da parte del Dipartimento per la giustizia minorile del Ministero della giustizia, quale autorità centrale, alle "informazioni contenute nelle banche dati in uso nell'ambito dell'esercizio delle loro attività istituzionali";

8) la legge 20 maggio 2016, n. 76, introduce nel nostro ordinamento la Regolamentazione delle unioni civili tra persone dello stesso sesso e disciplina delle convivenze. Tra le norme di interesse per l'Autorità si segnalano, in particolare, all'art. 1, comma 39, che in caso di malattia o di ricovero, estende ai conviventi di fatto il diritto reciproco di visita, di assistenza nonché di accesso alle informazioni personali, secondo le regole di organizzazione delle strutture ospedaliere o di assistenza pubbliche, private o convenzionate, previste per i coniugi e i familiari; il comma 55, secondo il quale il trattamento dei dati personali contenuti nelle certificazioni anagrafiche deve avvenire conformemente alla normativa prevista dal Codice, garantendo il rispetto della dignità dei soggetti che hanno sottoscritto il contratto di convivenza. La stessa disposizione stabilisce che "i dati personali contenuti nelle certificazioni anagrafiche non possono costituire elemento di discriminazione a carico delle parti del contratto di convivenza".

2.1.2. I decreti legislativi

Nel 2016 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 della l. 7 agosto 2015, n. 124, con la quale il Parlamento ha delegato il Governo ad intervenire in materia di riorganizzazione dello Stato e degli altri organismi pubblici al fine di razionalizzare il sistema e prevedere forme di semplificazione amministrativa:

1) il decreto legislativo 25 maggio 2016, n. 97, entrato in vigore il 23 giugno 2016, recante revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, che modifica la l. 6 novembre 2012, n. 190, disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione ed il d.lgs. 14 marzo 2013, n. 33, finalizzato a rafforzare la trasparenza amministrativa. Al riguardo il decreto ha inteso: ridefinire l'ambito di applicazione degli obblighi e delle misure in materia di trasparenza; prevedere misure organizzative per la pubblicazione di alcune informazioni e per la concentrazione e la riduzione degli oneri gravanti in capo alle amministrazioni pubbliche ed ai soggetti tenuti alla relativa osservanza; razionalizzare e precisare gli obblighi di pubblicazione; individuare i soggetti competenti all'irrogazione delle sanzioni per la violazione degli obblighi di trasparenza.

Di particolare interesse in materia di trattamento dei dati personali l'art. 3 che, nel novellare l'art. 2, d.lgs. n. 33/2013, introduce la libertà di accesso di chiunque ai dati e documenti detenuti dalla p.a., garantita, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, tramite l'accesso civico e la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pp.aa. e dei soggetti ai quali si estende la disciplina sul modello del *Freedom of information act* (Foia) dei sistemi anglosassoni. Particolare rilievo assume, inoltre, anche l'art. 4, che modifica l'art. 3 del d.lgs. n. 33/2013. Anche in questo caso si specifica che chiunque ha diritto di conoscere non soltanto i dati oggetto di pubblicazione obbligatoria, ma anche quelli oggetto di accesso civico. Vengono inoltre introdotti due ulteriori commi: il comma 1-*bis* volto a prevedere che, qualora siano coinvolti dati personali l'Anac, sentito il Garante, con propria delibera, adottata previa consultazione pubblica, possa identificare i dati, le informazioni e i

documenti oggetto di pubblicazione obbligatoria, per i quali la pubblicazione in forma integrale è sostituita con quella di informazioni riassuntive. Il comma 1-*ter* introduce una sorta di "clausola di flessibilità", prevedendo in capo all'Anac, in sede di Piano nazionale anticorruzione, il potere di "precisare" gli obblighi di pubblicazione e le relative modalità di attuazione in relazione alla natura dei soggetti, alla loro dimensione organizzativa e alle attività svolte.

L'art. 6, che sostituisce interamente il previgente art. 5, reca disposizioni in materia di dati pubblici aperti e accesso civico, prevedendo per chiunque indipendentemente dalla titolarità di situazioni giuridicamente rilevanti, la possibilità di accedere a tutti i dati detenuti dalle pp.aa., nel rispetto di alcuni limiti tassativamente indicati dalla legge. Si tratta, dunque, di un regime di accesso più ampio di quello previsto dalla versione originaria dell'art. 5 del d.lgs. n. 33/2013, in quanto consente di accedere non solo ai dati e documenti per i quali esistono specifici obblighi di pubblicazione ma anche ai dati per i quali non esiste tale obbligo. La richiesta di accesso non richiede alcuna qualificazione e motivazione, per cui il richiedente non deve dimostrare di essere titolare di un "interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso", così come stabilito invece per l'accesso ai sensi della legge sul procedimento amministrativo (l. n. 241/1990). Vengono, inoltre, introdotti due ulteriori articoli: l'art. 5-*bis*, il quale individua in modo puntuale gli interessi (pubblici e privati) a tutela dei quali è possibile rifiutare la richiesta di accesso civico (ad es., interessi pubblici inerenti, tra gli altri, la sicurezza pubblica o nazionale; il segreto di Stato; interessi privati inerenti, tra gli altri, la protezione dei dati personali e la libertà e la segretezza della corrispondenza) e l'art. 5-*ter*, che disciplina l'accesso per fini scientifici ai dati elementari raccolti per finalità statistiche. Dal punto di vista oggettivo i limiti applicabili alla nuova forma di accesso (di cui al nuovo art. 5-*bis*, d.lgs. n. 33/2013) sono più ampi e dettagliati rispetto a quelli indicati dall'art. 24, l. 7 agosto 1990, n. 241, in quanto consente alle amministrazioni di impedire l'accesso nei casi in cui questo possa compromettere rilevanti interessi pubblici generali (cfr. par. 4.3.1). Il decreto prevede, inoltre, una serie di modifiche alla disciplina sull'accesso alle informazioni pubblicate sui siti istituzionali (art. 9 che modifica l'art. 9, d.lgs. n. 33/2013) allo scopo di rendere agevole l'accesso ai dati e ai documenti pubblicati dalle amministrazioni. Per evitare duplicazioni (e dunque confusione nei fruitori del servizio), la pubblicazione degli stessi, da effettuarsi nella sezione "Amministrazione trasparente", potrà essere sostituita da un collegamento ipertestuale alla sezione del sito in cui sono presenti i relativi dati, informazioni o documenti, assicurando comunque la qualità di tali informazioni. Analogamente le pp.aa. titolari di banche dati, i cui contenuti abbiano per oggetto dati, documenti e informazioni oggetto di pubblicazione obbligatoria, sono obbligate a renderle pubbliche in modo tale che tutti i soggetti a cui si applica il decreto legislativo potranno assolvere agli obblighi di pubblicazione attraverso l'indicazione sul sito, nella sezione "Amministrazione trasparente", del collegamento ipertestuale alle stesse banche dati.

Sullo schema di decreto il Garante ha reso parere il 3 marzo 2016 (n. 92, doc. web n. 4772830) rilevando come in materia di trasparenza necessiti un approccio equilibrato per evitare che i diritti fondamentali alla riservatezza e alla protezione dei dati possano essere gravemente pregiudicati da una diffusione, non adeguatamente regolamentata, di documenti che riportino delicate informazioni personali (cfr. par. 3.3.1). Occorre quindi tenere in considerazione i rischi per la vita privata e per la dignità delle persone interessate, che possono derivare da obblighi di pubblicazione sui siti istituzionali di dati personali non sempre indispensabili a fini della trasparenza. Rischi che emergono ancora di più in considerazione della delicatezza di

alcune informazioni e della loro facile reperibilità grazie ai motori di ricerca, di tal che un eccesso indiscriminato di pubblicità rischia, peraltro, di occultare informazioni realmente significative di contro ad altre del tutto inutili, così ostacolando il controllo diffuso sull'esercizio del potere e degenerando in una forma di sorveglianza massiva.

Le criticità sono state ribadite dal Presidente dell'Autorità che, in una audizione tenutasi il 6 aprile 2016 avente ad oggetto lo schema di decreto legislativo, pur riconoscendo che il d.lgs. n. 33 "ha segnato una tappa fondamentale nell'evoluzione del nostro ordinamento, superando compiutamente la segretezza quale principale forma di esercizio del potere, mutando anche l'idea del rapporto tra singolo e autorità: da autoritativo, burocratico e insindacabile a paritetico, partecipato e controllabile" (cfr. par. 3.2), ha affermato anche che "se priva di adeguati criteri discretivi, la divulgazione di un patrimonio informativo immenso e sempre crescente (quale quello delle pubbliche amministrazioni) rischia, infatti, di mettere in piazza spaccati di vita individuale la cui conoscenza è inutile ai fini del controllo sull'esercizio del potere ma, per l'interessato, può essere estremamente dannosa".

2) Il decreto legislativo 26 agosto 2016, n. 179, reca una serie di modifiche ed integrazioni al codice dell'amministrazione digitale (Cad), di cui al d.lgs. 7 marzo 2005, n. 82, al fine di promuovere e rendere effettivi i diritti di cittadinanza digitale di cittadini e imprese. Il menzionato decreto conferma la centralità dei diritti di cittadinanza digitale e della scelta operata dal legislatore del 2015 di riconoscere alle tecnologie dell'informazione e della comunicazione nei rapporti tra cittadini, imprese e pp.aa., il ruolo di strumento fondamentale per la promozione del processo di radicale riorganizzazione dell'amministrazione dello Stato.

Con la carta della cittadinanza digitale (l. 7 agosto 2015, n. 124) si riconoscono direttamente diritti a cittadini e imprese e si costituisce la base giuridica per implementare la piattaforma di accesso che, attraverso il Sistema pubblico d'identità digitale e l'Anagrafe nazionale della popolazione residente, permetterà ai cittadini di accedere in modo omogeneo ai servizi pubblici – ed a quelli degli operatori privati che aderiranno – con un unico nome utente e un'unica *password* (prenotazioni di visite mediche, iscrizioni a scuola, pagamento dei tributi).

Le nuove disposizioni si prefiggono lo scopo di coordinare la disciplina nazionale in materia di documenti informatici e firme elettroniche con quella europea e, in particolare, con il nuovo regolamento (UE) 910/2014 (eIDAS) del Parlamento europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno il quale abroga la direttiva 1999/93/CE, in modo da garantire ad un tempo maggior validità ed efficacia ai documenti informatici anche privi di firma elettronica e di rafforzare l'efficacia delle firme elettroniche diverse da quella digitale. Ulteriori scopi sono la razionalizzazione e semplificazione della disciplina in materia di trasmissione di dati e documenti informatici tra le amministrazioni e tra queste ultime e i privati; il rafforzamento del principio dell'*open data by default* e coordinamento della normativa vigente in materia di dati aperti con quella di matrice europea relativa all'accesso alle informazioni pubbliche; la riorganizzazione e razionalizzazione – anche al fine di garantirne il coordinamento con le norme europee – delle disposizioni in materia di identità digitale; l'istituzione del Punto unico telematico di accesso ai servizi pubblici; la semplificazione e razionalizzazione della disciplina del Sistema pubblico di connettività.

In materia di requisiti per la gestione e conservazione dei documenti informatici, si prevede che il sistema di gestione informatica dei documenti della p.a. assicuri la sicurezza e l'integrità del sistema, la corretta e puntuale registrazione di protocollo

dei documenti in entrata e in uscita, raccolga informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati e consenta l'accesso, in condizioni di sicurezza, alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di riservatezza e tutela dei dati personali. Tale sistema è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio competente, il responsabile del trattamento dei dati personali di cui all'art. 29 del Codice, ove designato, e il responsabile del sistema della conservazione dei documenti informatici, nella definizione e gestione delle attività di rispettiva competenza. Particolare rilievo, inoltre, assume l'art. 58 che modifica l'art. 73 del Cad, semplificando e razionalizzando in termini significativi la vigente disciplina sul Sistema pubblico di connettività. La nuova struttura e formulazione delle disposizioni disegna tale sistema come l'insieme di infrastrutture tecnologiche e di regole tecniche che assicura l'interoperabilità tra i sistemi informativi delle pp.aa., permettendo il coordinamento informativo e informatico dei dati tra le amministrazioni centrali, regionali e locali e tra queste e i sistemi dell'Unione europea. Viene, inoltre, prevista una generale apertura – previa istanza all'AgID – di tale sistema ai gestori di servizi pubblici e ai privati.

Il Garante, in data 9 giugno 2016, ha reso il proprio parere (n. 255, doc. web n. 5177397) sullo schema di decreto e in tale sede ha ritenuto opportuno, viste le significative innovazioni al Cad e visto il notevole impatto del provvedimento sui diritti delle persone, chiedere che venissero apprestate maggiori garanzie alla riservatezza di chiunque si avvalga dell'identità digitale (cfr. par. 3.3.1). Ha segnalato quindi la necessità di adeguare i termini utilizzati nello schema alle definizioni adottate nel citato regolamento eIDAS e di garantire coerenza tra decreti relativi a Cad, Spid e a trasparenza e anticorruzione; ha chiesto, poi, di estendere il diritto di avere e poter utilizzare un'identità digitale a chiunque risieda legalmente in Italia, non limitandola quindi, senza motivo, a soli cittadini e imprese e di garantire che l'elezione o l'assegnazione del domicilio digitale, considerato mezzo esclusivo di comunicazione con le pp.aa., resti nella facoltà dell'interessato e non divenga un obbligo. Il Garante ha chiesto, inoltre, di disporre, in linea con i princìpi di pertinenza e non eccedenza, adeguate garanzie per i dati personali, in particolare eliminando la possibilità di inserire nel certificato di firma elettronica qualificata dati aggiuntivi rispetto a quanto previsto dal regolamento eIDAS (ad es., il codice fiscale) e, in tema di sicurezza, ritiene opportuno non abrogare l'articolo relativo al *disaster recovery* e alla continuità operativa, mantenendo in capo ai soggetti pubblici l'obbligo di provvedere alla conservazione sicura dei dati anche nella fase di attuazione delle nuove regole.

3 I rapporti con il Parlamento e le altre Istituzioni

3.1. *Le audizioni del Garante in Parlamento*

Nel 2016 il Garante ha partecipato ad alcune audizioni presso Commissioni parlamentari e altri organismi anche bicamerali su temi di propria competenza all'esame del Parlamento, nell'ambito di indagini conoscitive o nel corso dei lavori per l'approvazione di progetti di legge, segnalandone i riflessi in materia di protezione dei dati personali. In questo quadro si collocano, in particolare:

a) un'audizione tenutasi il 22 novembre 2016 presso la Commissione lavoro e previdenza sociale del Senato in merito alle misure per prevenire e contrastare condotte di maltrattamento o di abuso, anche di natura psicologica, in danno dei minori negli asili nido e nelle scuole dell'infanzia e delle persone ospitate nelle strutture socio-sanitarie e socio-assistenziali per anziani e persone con disabilità e delega al Governo in materia di formazione del personale (doc. web n. 5696272);

b) un'audizione informale tenutasi il 16 novembre 2016, presso la Commissione lavori pubblici e comunicazioni del Senato, concernente le modifiche al Registro delle opposizioni e contrasto al *telemarketing* selvaggio (doc. web n. 5661956);

c) un'audizione tenutasi in data 22 settembre 2016, presso le Commissioni riunite affari costituzionali e giustizia della Camera, in merito alla comunicazione della Commissione al Parlamento europeo, al Consiglio europeo e al Consiglio recante l'attuazione dell'Agenda europea sulla sicurezza per combattere il terrorismo e la preparazione del terreno per l'Unione della sicurezza (COM(2016) 230) (doc. web n. 5447549);

d) un'audizione tenutasi il 27 luglio 2016 presso le Commissioni riunite affari costituzionali e lavoro della Camera, in relazione all'esame delle proposte di legge recanti norme in materia di videosorveglianza negli asili nido e nelle scuole dell'infanzia nonché presso le strutture socio-assistenziali per anziani, disabili e minori in situazione di disagio (doc. web n. 5301830);

e) un'audizione informale tenutasi il 12 luglio 2016, presso le Commissioni riunite trasporti, poste e telecomunicazioni e attività produttive commercio e turismo della Camera, nell'ambito dell'esame della proposta di legge in materia di disciplina delle piattaforme digitali per la condivisione di beni e servizi e disposizioni per la promozione dell'economia della condivisione (doc. web n. 5251866);

f) un'audizione tenutasi il 21 giugno 2016 presso il Comitato parlamentare per la sicurezza della Repubblica (Copasir), sul tema della sicurezza e della *privacy*;

g) un'audizione informale, tenutasi il 6 aprile 2016 presso le Commissioni congiunte affari costituzionali del Senato e della Camera, riguardo allo schema di decreto legislativo correttivo della disciplina di trasparenza della pubblica amministrazione (doc. web n. 4861875);

h) un'audizione tenutasi il 16 marzo 2016 presso le Commissioni riunite trasporti e lavoro della Camera, in tema di mercato unico digitale e commercio elettronico (doc. web n. 4789144);

i) un'audizione tenutasi l'8 marzo 2016 presso la Commissione affari sociali della Camera nell'ambito dell'esame delle proposte di legge recanti istituzione e disciplina del registro nazionale e dei registri regionali dei tumori (doc. web n. 4762078).

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, sono stati forniti elementi di valutazione, ai fini della risposta da parte del Governo, su:

a) un'interrogazione a risposta orale concernente la distruzione del materiale cartaceo contenente dati sensibili (n. 3/02617 dell'On. Fravezzi – nota 7 settembre 2016);

b) un'interpellanza urgente concernente eventuali iniziative del Governo a tutela del consumatore, finalizzate alla regolamentazione e alla limitazione del cd. *click-bait*, pratica consistente nell'attirare gli utenti in modo fraudolento su pagine web a contenuto commerciale durante la navigazione in internet (n. 2/01413 dell'On. Coppola ed altri – nota 12 luglio 2016);

c) un'interpellanza concernente il canone Rai in bolletta (n. 2/01404, dell'On. Di Battista – nota 1° luglio 2016);

d) un'interrogazione a risposta scritta riguardante il trattamento dei dati in riferimento agli atti di iniziativa popolare EU (n. 4/12986, dell'On. Fraccaro – nota 28 aprile 2016);

e) un'interrogazione a risposta scritta riguardante la riservatezza delle comunicazioni dei parlamentari (n. 4/05507 dell'on. Gasparri – nota 22 aprile 2016);

f) un'interrogazione a risposta immediata (*question time*), dell'On. Vezzali, riguardante la videosorveglianza negli istituti scolastici e nei luoghi di cura (nota 5 aprile 2016);

g) un'interrogazione a risposta orale concernente la riservatezza delle comunicazioni elettroniche dei parlamentari (n. 3/02652 degli On.li Capacchione ed Esposito – nota 29 marzo 2016);

h) un'interrogazione a risposta scritta, relativa alla pubblicazione di dati dei dipendenti Ilva su di un portale aziendale (n. 4/11767 dell'on. Petraroli – nota 11 febbraio 2016);

i) un'interrogazione a risposta scritta concernente le attività di *telemarketing* e i *call center* (n. 5/06907 dell'On. Albanella – nota del 28 gennaio 2016).

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 Presidente del Consiglio dei ministri di concerto con il Ministro dell'istruzione, recante disciplina delle modalità di assegnazione e utilizzo della Carta elettronica per l'aggiornamento e la formazione del docente di ruolo delle istituzioni scolastiche di ogni ordine e grado (parere 16 novembre 2016, n. 487, doc. web n. 5757175);

2) regolamento del Ministro della salute recante norme in materia di manifestazione della volontà di accedere alle tecniche di procreazione medicalmente assistita, in attuazione dell'art. 6, comma 3, della l. 19 febbraio 2004, n. 40 (parere 10 novembre 2016, n. 468, doc. web n. 5763307);

3) schema di convenzione della Presidenza del Consiglio dei ministri – AgID per l'adesione al sistema pubblico per la gestione dell'identità digitale (Spid) per i privati fornitori di servizi (parere 29 settembre 2016, n. 378, doc. web n. 5558208);

4) schema di provvedimento del Direttore dell'Agenzia delle entrate in tema di modalità tecniche di utilizzo ai fini della dichiarazione dei redditi precompilata dei dati delle spese sanitarie e delle spese veterinarie (parere 28 luglio 2016, n. 334, doc. web n. 5407586);

5) schema di decreto della Ragioneria dello Stato in materia di trasmissione telematica dei dati delle spese sanitarie sostenute, a partire dal l° gennaio 2016, presso strutture autorizzate (e non accreditate) per l'erogazione dei servizi sanitari (parere 28 luglio 2016, n. 333, doc. web n. 5407516);

6) schema di decreto del Ministero dell'economia e delle finanze con il quale vengono definiti i termini e le modalità per la trasmissione telematica all'Agenzia delle entrate dei dati relativi alle spese sanitarie diverse da quelle previste dal d.lgs. n. 175/2014 e alle spese veterinarie (parere 28 luglio 2016, n. 332, doc. web n. 5407413);

7) schema di decreto della Ragioneria dello Stato in materia di trasmissione di nuove tipologie di spese sanitarie e veterinarie sostenute dai cittadini a partire dal 1° gennaio 2016 (parere 28 luglio 2016, n. 331, doc. web n. 5407377;

8) decreto del Ministro dell'interno di concerto con il Ministro della giustizia di attuazione dell'art. 3, comma 9, d.P.R. 7 aprile 2016, n. 87, recante l'istituzione della banca dati dna (parere 28 luglio 2016, n. 330, doc. web n. 5387695);

9) decreto del Ministro della giustizia in materia di tenuta e aggiornamento degli albi, degli elenchi e dei registri da parte dei Consigli dell'ordine degli avvocati (parere 28 luglio 2016, n. 329, doc. web n. 5385546);

10) decreto del Presidente del Consiglio dei ministri recante criteri e modalità di attribuzione e utilizzo della carta elettronica *ex* art.1, comma 979, l. 28 dicembre 2015, n. 208 e successive modificazioni (parere 28 luglio 2016, n. 328, doc. web n. 5387638);

11) decreto del Presidente del Consiglio dei ministri recante il regolamento concernente la determinazione dell'età dei minori non accompagnati vittime di reato (parere 13 luglio 2016, n. 301, doc. web n. 5320151);

12) schemi di provvedimento dell'Agenzia delle entrate in materia di *compliance* fiscale internazionale e normativa FATCA - *Foreign Account Tax Compliance Act* (parere 6 luglio 2016, n. 289, doc. web n. 5387587);

13) decreti del Ministro dell'istruzione, dell'università e della ricerca relativi alle modalità e ai contenuti delle prove di ammissione ai corsi di laurea magistrale a ciclo unico ad accesso programmato a livello nazionale a.a. 2016/2017 (parere 30 giugno 2016, n. 284, doc. web n. 5387469);

14) decreto del Ministro dell'istruzione, dell'università e della ricerca integrativo al d.m. 25 gennaio 2016, n. 24 – Anagrafe nazionale studenti – inclusione settore dell'infanzia (parere 12 maggio 2016, n. 215, doc. web n. 5029436);

15) decreto del Ministro dello sviluppo economico di attuazione dell'art. 1, comma 154, l. 28 dicembre 2015, n. 208 (legge di stabilità) – canone Rai in bolletta (parere 27 aprile 2016, n. 192, doc. web n. 4943860);

16) decreto del Ministro dell'istruzione, dell'università e della ricerca di modifica al decreto ministeriale n. 74/2010 in materia di Anagrafe nazionale studenti (Ans) Trattamento dati sui percorsi scolastici, formativi e in apprendistato dei singoli studenti e loro valutazione (parere 21 aprile 2016, n. 177, doc. web n. 5029548);

17) protocollo del Ministero dell'economia e delle finanze concernente i flussi di dati che possono essere trasmessi al Ministero della salute e alle Regioni (tessera sanitaria) (parere 10 marzo 2016, n. 108, doc. web n. 4943801);

18) convenzione fra l'Agenzia per l'Italia digitale (AgID) ed i gestori di identità digitale, da adottare ai sensi dell'art.10, comma 2, d.P.C.M. 24 ottobre 2014 recante la definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (Spid) (parere 18 febbraio 2016, n. 62, doc. web n. 4797918);

19) decreto del Ministro dei beni e delle attività culturali e del turismo, recante il regolamento di attuazione dell'art. 85, d.lgs. n. 42 del 22 gennaio 2004 (codice dei beni culturali e del paesaggio) al fine di individuare specifiche modalità di realizzazione di una banca dati di beni culturali illecitamente sottratti (parere 4 febbraio 2016, n. 33, doc. web n. 4727696);

20) provvedimento della Ragioneria dello Stato, volto a disciplinare le modalità di accesso alle spese sanitarie e relativa opposizione (provv. 4 febbraio 2016, n. 23, doc. web n. 4797834).

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 aventi rango primario.

È stato richiesto il parere formale del Garante sullo schema di decreto legislativo recante modifiche e integrazioni al codice dell'amministrazione digitale di cui al d.lgs. 7 marzo 2005, n. 82, ai sensi dell'art. 1 della l. 7 agosto 2015, n. 124 in materia di riorganizzazione delle amministrazioni pubbliche (parere 9 giugno 2016, n. 255, doc. web n. 5177397);

È stato altresì richiesto parere sullo schema di decreto legislativo recante revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della l. 6 novembre 2012, n. 190 e del d.lgs. 14 marzo 2013, n. 33, ai sensi dell'art. 7 della l. 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche (parere 3 marzo 2016, n. 92, doc. web n. 4772830). Al riguardo occorre considerare che l'art. 154, comma 4, del Codice fa riferimento alla normativa avente rango secondario, anche se la correlata disposizione della direttiva europea non reca una distinzione al riguardo (art. 28, par. 2). Le richieste di parere su atti primari si inquadrano oggi in un contesto di collaborazione con le amministrazioni interessate che l'Autorità, come più volte segnalato alla Presidenza del Consiglio dei ministri, auspica possa ulteriormente svilupparsi, nella consapevolezza che sia di grande utilità il coinvolgimento del Garante nella fase preparatoria di iniziative legislative, oltre che regolamentari, del Governo al fine di valutarne previamente l'impatto sulla protezione dei dati personali e sui diritti delle persone. Ciò anche alla luce del nuovo regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, entrato in vigore il 24 maggio 2016 e che sarà immediatamente applicabile in tutti gli Stati membri dell'Unione europea a decorrere dal 25 maggio 2018.

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, nel corso dell'anno, ha esaminato 11 leggi regionali e, in linea gene-

rale, ha riscontrato un sostanziale corretto svolgimento della potestà legislativa regionale in relazione agli aspetti di protezione dei dati personali, salvo quanto di seguito esposto. Alcuni interventi hanno riguardato la già nota problematica delle implicazioni che possono derivare da iniziative legislative regionali che introducano obblighi di diffusione di dati personali nuovi e/o ulteriori rispetto a quelli già previsti dalla normativa statale in materia di trasparenza.

In un primo caso il Garante ha ritenuto necessario formulare alla Presidenza del Consiglio dei ministri talune osservazioni in merito alla compatibilità della legge della Regione Trentino Alto Adige n. 30/2015 recante nuove norme relative alla pubblicazione e alla diffusione del Bollettino ufficiale della Regione autonoma Trentino Alto Adige con le norme costituzionali ed i princìpi in materia di protezione dei dati personali. Ciò in quanto il nuovo regime di pubblicità, come disciplinato dal legislatore regionale, introduceva un'ampia e indeterminata possibilità di diffusione di provvedimenti contenenti anche dati personali, non conforme alle esclusioni o limitazioni già previste da normative nazionali di settore. Le stesse previsioni in materia di tutela della riservatezza e di protezione dei dati personali, limitate nella legge regionale al rispetto dei soli princìpi di pertinenza, indispensabilità, necessità e non eccedenza di cui al Codice, comportavano una sua modifica o applicazione selettiva nonostante la Regione non abbia una tale competenza legislativa, essendo la materia della protezione dei dati personali di esclusiva attribuzione statale (art. 117, comma 2, lett. *l*), Cost.). Con successiva nota del 3 febbraio 2016 il vicepresidente della Regione ha comunicato alla Presidenza del Consiglio dei ministri l'impegno del governo regionale ad emendare la legge secondo le osservazioni del Garante.

Analoghe criticità sono emerse nell'esame della legge della Provincia di Bolzano n. 9/2016, recante modifiche alla legge provinciale n. 17 del 22 ottobre 1993 – disciplina del procedimento amministrativo e del diritto di accesso ai documenti amministrativi che introduce nuovi obblighi di pubblicità – tramite la pubblicazione nell'albo *online* della provincia – di atti e provvedimenti non previsti da disposizioni legislative, laddove gli stessi interessino la generalità dei cittadini o determinate categorie di soggetti. Al riguardo, il Garante ha rappresentato alla Presidenza del Consiglio dei ministri che il semplice richiamo, effettuato dal legislatore provinciale, al necessario rispetto "dei princìpi e dei limiti stabiliti dalla normativa in materia di protezione dei dati personali" non fosse idoneo a superare le criticità, tenuto conto che il Codice ammette la diffusione dei dati personali da parte dei soggetti pubblici solo in presenza di una norma di legge o di regolamento (art. 19, comma 3). Infine, ulteriori criticità hanno riguardato le disposizioni in materia di dati aperti e riutilizzo, laddove si prevede che l'amministrazione debba assicurare la diffusione dei dati pubblici e dei documenti contenenti dati pubblici in formati di tipo aperto e liberamente accessibili a tutti, anche se nel rispetto della normativa sull'accesso agli atti amministrativi, sulla protezione dei dati personali e sul diritto alla protezione intellettuale e industriale. Le controdeduzioni formulate dalla Provincia di Bolzano non sono state ritenute atte a superare le criticità evidenziate, che sono state pertanto ribadite alla Presidenza del Consiglio dei ministri.

Sempre in materia di trasparenza, il Garante è altresì intervenuto formulando osservazioni alla Presidenza del Consiglio dei ministri in relazione alla legge della Regione Lazio n. 17/2016, recante legge di stabilità regionale 2017 che, all'art. 3, comma 67, in contrasto con l'art. 19 del Codice, introduce un nuovo obbligo di pubblicità relativo a soggetti destinatari di contributi economici laddove prevede la pubblicazione da parte della direzione regionale competente in materia di cultura dell'elenco dei soggetti ammissibili al contributo, mentre la legislazione statale di

settore in materia di trasparenza stabilisce l'obbligo di pubblicazione dei soli atti di concessione delle sovvenzioni, contributi, sussidi e altro, pubblicazione che costituisce condizione legale di efficacia dei provvedimenti che dispongono concessioni ed attribuzioni di importo complessivo superiore ai mille euro nel corso dell'anno solare al medesimo beneficiario (art. 26, commi 2 e 3, d.lgs. n. 33/2013).

Il Garante ha poi segnalato alla Presidenza del Consiglio dei ministri di aver rilevato profili di possibile illegittimità riferiti alla legge della Regione Calabria n. 2/2016 recante istituzione del Registro tumori della popolazione della Regione Calabria. In particolare, l'Autorità ha evidenziato la mancanza di espressa definizione delle specifiche finalità che possono giustificare il trattamento dei dati sanitari necessari alla tenuta ed al funzionamento del registro tumori, nonché la definizione dei tipi di dati trattati e delle operazioni eseguibili, discendenti dal rispetto dei princìpi di proporzionalità, pertinenza e non eccedenza in relazione alle finalità, necessità ed indispensabilità dei dati trattati.

Con successiva nota il Presidente della Regione Calabria ha comunicato alla Presidenza del Consiglio dei ministri l'impegno del Governo regionale a presentare un nuovo disegno di legge appositamente emendato secondo le indicazioni del Garante. Con la l. 20 aprile 2016, n. 12 tali modifiche ed integrazioni sono state adottate dalla Regione.

Il Garante è altresì intervenuto in merito alla legittimità costituzionale della legge della Regione Abruzzo n. 2/2016, nella parte recante modifiche alla l.r. 10 agosto 2010, n. 40 (Testo unico delle norme sul trattamento economico spettante ai Consiglieri regionali e sulle spese generali di funzionamento dei gruppi consiliari). In questo ambito il Garante, ribadendo l'importanza della diffusione delle informazioni per finalità di trasparenza e il fatto che la disciplina in materia di protezione dei dati personali non costituisca ostacolo alla pubblicità dell'azione pubblica, ha rammentato come ciò debba avvenire nel rispetto della dignità e dei diritti fondamentali della persona, quali quello alla riservatezza e alla protezione dei dati personali. In particolare, in materia di vitalizi e di assegni di reversibilità, il Garante ha avuto modo di precisare ancora una volta come "le pubbliche amministrazioni. non sono libere di diffondere dati personali ulteriori, non individuati dal d.lgs. n. 33/2013 o da altra specifica norma di legge o di regolamento (art.19, comma 3, del Codice), e che l'eventuale pubblicazione di dati, informazioni e documenti, che non si ha l'obbligo di pubblicare, è legittima solo procedendo alla anonimizzazione dei dati personali eventualmente presenti (art. 4, comma 3, d.lgs. n. 33/2013)".

In riferimento alla legge della Regione Sicilia n. 7/2016, recante disciplina dei contenuti formativi per l'esercizio delle attività di subacquea industriale, il Garante ha rilevato che per l'iscrizione al Repertorio telematico dei soggetti formati si chiede di fornire "l'autorizzazione al trattamento e alla pubblicazione dei dati personali", laddove la raccolta dei dati personali ai fini dell'iscrizione nel Repertorio e la loro diffusione configurano un trattamento di dati in ambito pubblico il cui presupposto di liceità non deve essere individuato nel consenso dell'interessato, bensì nella necessità del trattamento di tali informazioni per le funzioni istituzionali di gestione e tenuta del Repertorio telematico nonché – per quanto riguarda la loro diffusione – nelle disposizioni della medesima legge che prevedono la pubblicazione *online* di tale elenco. Peraltro è stata segnalata la mancanza, all'atto dell'istanza di iscrizione nel Repertorio, di una previsione relativa ad "un'idonea informativa sul trattamento dei dati personali ai sensi dell'art. 13, d.lgs. n. 196/2003" in modo da consentire agli interessati di acquisire piena consapevolezza di tutti gli aspetti del trattamento dei dati personali connesso all'iscrizione nel Repertorio.

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 pubbliche amministrazioni*

Nell'anno di riferimento il Garante ha dato parere favorevole sullo schema di regolamento per i trattamenti dei dati sensibili e giudiziari effettuati dall'Agenzia nazionale per i giovani (di seguito Agenzia), che ha tenuto conto delle indicazioni formulate dal Garante in occasione dei numerosi contatti, anche informali. È stata, in particolare, oggetto di attenzione la valutazione del rapporto tra i dati che l'Agenzia intende trattare e gli adempimenti ad essa spettanti nell'ottica del più rigoroso rispetto del principio di indispensabilità (art. 22, commi 3 e 5, del Codice), "fermo restando che le operazioni di raffronto e interconnessione con base dati di diversi titolari sono ammesse solo se previste da espressa disposizione di legge" (cfr. art. 22, commi 10 e 11, del Codice) (provv. 4 febbraio 2016, n. 34, doc. web n. 4842686).

Il Garante ha, altresì espresso parere favorevole sul nuovo regolamento per il trattamento dei dati sensibili e giudiziari effettuati dall'Autorità garante della concorrenza e del mercato (Agcm), che abroga e sostituisce il precedente. L'esigenza di aggiornamento è derivata dall'ampliamento delle competenze attribuite all'Agcm nell'ambito della tutela della concorrenza e del *rating* di legalità delle imprese (art. 5-*ter,* d.l. 24 gennaio 2012, n. 1, convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 24 marzo 2012, n. 27). La revisione del regolamento assicura una maggiore chiarezza anche dal punto di vista sistematico al trattamento di dati giudiziari per finalità di attribuzione del *rating* di legalità alle imprese da parte dell'Agcm. Nel corso dell'istruttoria, inoltre, l'Agcm ha individuato, su indicazione del Garante, specifiche garanzie per gli interessati, quali, in particolare, l'inserimento di un avviso in ordine all'informativa da fornire agli interessati nel formulario da compilarsi a cura delle società richiedenti l'attribuzione di *rating*, anche al fine di evitare criticità in caso di diniego del *rating* a causa dell'esistenza di precedenti penali a loro carico (provv. 9 giugno 2016, n. 257, doc. web n. 5270614).

Sempre con riguardo ai trattamenti di dati sensibili e giudiziari presso le pp.aa., merita segnalare il quesito formulato dalla prefettura - UTG di Potenza con riferimento alla possibilità di comunicare a una società di trasporto pubblico locale le motivazioni alla base di un provvedimento sanzionatorio di sospensione della patente di guida nei confronti di un dipendente della stessa, con mansioni di conducente di autobus di linea, per violazione dell'art. 75, d.P.R. n. 309/1990 (testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza). Il Garante si è espresso stabilendo che, nel caso di sospensione della patente, non è prevista la comunicazione da parte della prefettura "degli accertamenti e degli atti" al datore di lavoro del soggetto sanzionato. La sanzione, infatti, era stata comminata a seguito di un articolato procedimento avanti al Prefetto che ha previsto, tra l'altro, la contesta-

zione immediata, l'esame tossicologico delle sostanze sequestrate, il ritiro e la trasmissione al Prefetto della patente da parte delle Forze dell'ordine che hanno provveduto all'accertamento, la convocazione dell'interessato avanti al Prefetto, l'invito a partecipare a specifici programmi (art. 75, commi 1-5, cit.). La medesima disposizione prevede altresì che degli "accertamenti e degli atti di cui ai commi da 1 a 5 può essere fatto uso soltanto ai fini dell'applicazione delle misure e delle sanzioni previste nel presente articolo e nell'art. 75-*bis*" (art. 75, comma 6, cit.). Conformemente al predetto quadro normativo, il regolamento sul trattamento dei dati sensibili e giudiziari del Ministero dell'interno prevede la comunicazione di dati personali unicamente ai seguenti soggetti: "Servizi pubblici per le tossicodipendenze, Forze di polizia segnalanti per lo svolgimento degli adempimenti connessi alle procedure previste dagli artt. 75 e 121 del d.P.R. 309/90" (cfr. decreto 21 giugno 2006, n. 244, scheda n. 24, applicazione normativa antidroga). Ciò, tenuto conto che, per le finalità di salvaguardia della vita e dell'incolumità del lavoratore e della collettività, la società di trasporto, a conoscenza del provvedimento di sospensione della patente del dipendente, può senz'altro attivare, gli strumenti di sorveglianza sanitaria previsti dalla normativa sulla tutela della salute e della sicurezza sui luoghi di lavoro, la quale prevede che "le visite mediche (…) comprendono gli esami clinici e biologici e indagini diagnostiche mirati al rischio ritenuti necessari dal medico competente. Nei casi ed alle condizioni previste dall'ordinamento, le visite (…) sono altresì finalizzate alla verifica di assenza di condizioni di alcol dipendenza e di assunzione di sostanze psicotrope e stupefacenti" (art. 41, d.lgs. 9 aprile 2008, n. 81), oppure da altre disposizioni che prevedono accertamenti specifici per i lavoratori destinati a mansioni che comportano elevati rischi di infortunio ovvero rischi per la sicurezza, la incolumità e la salute dei terzi (cfr. art. 125, d.P.R. n. 309/1990; art. 15, l. n. 125/2001) (nota 2 novembre 2016).

Banca dati integrata sull'assistenza socio-sanitaria

Il Garante si è inoltre pronunciato sulle modifiche al regolamento per il trattamento dei dati sensibili e giudiziari predisposte dalla Regione Emilia-Romagna in relazione alle attività di assistenza socio-sanitaria a favore di fasce deboli di popolazione effettuate dalle strutture sanitarie (provv. 5 maggio 2016, n. 203, doc. web n. 5185386). Le modifiche hanno riguardato, in particolare, la scheda del regolamento regionale (30 maggio 2014, n. 1) predisposto a suo tempo (cfr. scheda n. 6 dell'All. B) in conformità allo schema tipo di regolamento elaborato dalla Conferenza delle regioni e delle province autonome, sul quale il Garante aveva reso parere favorevole (parere 26 luglio 2012, n. 220, doc. web n. 1915390). Le integrazioni, sottoposte alla valutazione dell'Autorità, hanno riguardato la possibilità, prevista dagli accordi di integrazione socio-sanitaria in attuazione dei piani di zona ed in conformità alla legislazione regionale in materia, per le ausl e i comuni, afferenti allo stesso distretto sanitario, di costituire una banca dati integrata sull'assistenza socio-sanitaria. I dati sensibili e giudiziari indispensabili alla presa in carico delle persone che accedono ai servizi sociali territoriali e necessitano di seguire un percorso socio-sanitario integrato sarebbero così raccolti in un archivio informatizzato unico, al fine di consentire la gestione integrata dei processi assistenziali in parola. Riguardo alla banca dati, di cui sono contitolari le ausl e i comuni appartenenti allo stesso ambito distrettuale, l'Autorità, nel parere citato, ha chiesto di definire le responsabilità, in ordine all'osservanza degli obblighi in materia di protezione dei dati personali, di ciascuno degli enti coinvolti nel trattamento, specie quelli riguardanti l'informativa e l'esercizio dei diritti degli interessati. Tale accorgimento è volto, in particolare, a evitare che la scelta della contitolarità porti a una confusa e impraticabile ripartizione delle responsabilità conseguenti al trattamento delle informazioni, minando così l'efficacia della normativa sulla protezione dei dati personali. Inoltre, in ottemperanza al

principio di semplificazione, l'Autorità ha disposto che i comuni della Regione che, nell'ambito degli accordi di integrazione socio-sanitaria, intendano costituire una banca dati integrata, insieme alle ausl del distretto, dovranno aggiornare i propri atti regolamentari, al fine di effettuare lecitamente i trattamenti di dati sensibili ad essa correlati, per il perseguimento delle specifiche finalità di assistenza socio-sanitaria. Ciò, senza dover richiedere singolarmente all'Autorità un nuovo parere ai sensi degli artt. 20, comma 2, e 21, comma 2, del Codice, sempreché tali trattamenti siano effettuati in conformità alle previsioni di integrazione regolamentare sottoposte al vaglio del Garante.

Sistema informativo "fragilità"

Tra i trattamenti di dati sensibili effettuati nell'ambito delle attività di assistenza socio-sanitaria, nel regolamento regionale, è stato previsto anche un nuovo sistema informativo denominato "fragilità". Il sistema, oggetto di sperimentazione nell'ambito delle iniziative finanziate dal "fondo regionale non autosufficienza" (delibera della Giunta regionale 30 luglio 2007, n. 1206), è finalizzato alla prevenzione e al monitoraggio delle situazioni di fragilità in cui versano taluni soggetti identificati come non autosufficienti o a rischio di non autosufficienza. Esso mira a identificare precocemente la popolazione fragile, a stratificarla sulla base di profili di rischio e a monitorare gli interventi di assistenza socio-sanitaria attraverso la raccolta, in un'unica banca dati, di informazioni anagrafiche, sanitarie, reddituali, nonché riguardanti il censimento dell'Istat e l'assegnazione di immobili di edilizia pubblica. Al riguardo, il Garante ha evidenziato che se la costituzione e la gestione di tale sistema informativo comporta, come sembra, trattamenti automatizzati di dati sensibili volti a definire il profilo o la personalità degli interessati, utilizzando banche dati di diversi titolari, per legittimare l'utilizzo di tali delicate categorie di informazioni, è necessario individuare un idoneo presupposto legislativo (art. 22, comma 11, del Codice). Anche se la profilazione è finalizzata ad arrecare benefici agli interessati non può, infatti, escludersi che, a causa di essa, singoli individui siano ingiustamente privati di questi servizi o vengano esposti a rischi di discriminazione. Ciò, in considerazione del fatto che, nella definizione del profilo dell'interessato, sono utilizzate informazioni particolarmente delicate riguardanti non solo la salute, ma anche lo stato di indigenza o di disagio familiare e sociale. Per tali ragioni, la disciplina sulla protezione dei dati personali ammette la profilazione degli interessati con dati sensibili, soltanto nella misura in cui ciò sia previsto dalla legge e subordina questo tipo di trattamento all'adozione di idonee garanzie, con particolare riferimento al diritto di opposizione per motivi legittimi (art. 14, comma 2, del Codice e raccomandazione del Consiglio d'Europa Rec (2010)13 sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione). Non essendo stato possibile rinvenire i necessari presupposti di legge che consentirebbero di trattare lecitamente i predetti dati personali, si è chiesto pertanto alla Regione di espungere le modifiche al regolamento regionale riguardanti il sistema informativo "fragilità".

4.2. *Vigilanza sulle grandi banche dati pubbliche*

L'Autorità ha proseguito anche nel 2016 l'attività di vigilanza sulle grandi banche dati pubbliche procedendo sia d'ufficio che in seguito a specifiche segnalazioni o comunicazioni relative a violazioni di sicurezza (*data breach*) inviate direttamente dalle pp.aa. in linea con il provvedimento 2 luglio 2015, n. 393 (doc. web n. 4129029). Con tale provvedimento il Garante, anticipando quanto diverrà obbligatorio ai sensi dell'art. 33 del regolamento (UE) 2016/679, ha ritenuto necessario

assoggettare il trattamento dei dati personali, effettuato nell'ambito delle banche dati delle amministrazioni pubbliche, all'obbligo di comunicazione al Garante del verificarsi di violazioni dei dati o incidenti informatici (accessi abusivi, azione di *malware*) che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione. Le pp.aa. sono pertanto tenute a comunicare al Garante, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati (cd. *data breach*).

Nel 2016 sono pervenute 15 comunicazioni di *data breach*, da parte di diverse categorie di soggetti pubblici le cui istruttorie hanno portato l'amministrazione, anche su indicazione del Garante, a introdurre misure di sicurezza aggiuntive a quelle già predisposte e, in alcuni casi (5), all'invio di segnalazioni alle competenti Procure della Repubblica per violazione delle misure minime di sicurezza o accesso abusivo al sistema informatico, ai sensi dell'art. 615-*ter* del codice penale.

In diversi casi (8) le istruttorie effettuate sulla base di segnalazioni e reclami hanno consentito di accertare accessi ingiustificati alle grandi banche dati pubbliche (Inps e Anagrafe tributaria) da parte di dipendenti o altri soggetti autorizzati (per lo più personale operante presso patronati). Occorre considerare che, come stabilito dalla sentenza delle sez. unite penali della Corte di cassazione n. 4694/2012, "integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-*ter* c.p., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso". Anche in questi casi quindi, una volta individuate le credenziali utilizzate per gli accessi (attraverso l'analisi dei *file* di *log* dei sistemi) e l'assenza di una oggettiva giustificazione degli stessi, si è proceduto alla trasmissione degli atti alla Procura delle Repubblica competente per le valutazioni in ordine alla sussistenza del reato di accesso abusivo.

Sul tema del controllo degli accessi alle grandi banche dati pubbliche, oggetto di particolare attenzione dell'Autorità, sono state profuse rilevanti energie anche sotto il profilo preventivo. Sono infatti proseguite, anche nel 2016, le verifiche volte ad accertare l'adeguatezza delle misure a protezione degli accessi all'Anagrafe tributaria.

In tale contesto, il Garante, in collaborazione con il Nucleo speciale della Guardia di finanza, ha compiuto un ciclo ispettivo nei confronti dei centri di assistenza fiscale (Caf), verificando, in particolare, gli accessi alla cd. dichiarazione precompilata su delega degli interessati, al fine di verificare, in particolare, le funzionalità del sistema informatico utilizzato in questo ambito dall'Agenzia delle entrate (denominato Entratel) per verificare la gestione degli utenti, le modalità di trattamento delle dichiarazioni precompilate scaricate, le modalità di acquisizione e registrazione delle deleghe dei contribuenti, nonché le modalità di accesso alle certificazioni uniche rilasciate dall'Inps.

Dall'esame delle risultanze di tale attività, si è rilevata la necessità di prevedere misure di sicurezza integrative per l'accesso alla dichiarazione precompilata da parte degli intermediari (cfr. par. 4.6) e sono state definite, da parte dell'Inps, modalità rafforzate per il rilascio delle certificazioni uniche ai Caf.

Con riferimento alle banche dati pubbliche e all'individuazione delle relative modalità di accesso, il Garante ha reso il parere di competenza sullo schema di d.P.C.M. attuativo dell'art. 1, comma 979, della l. 28 dicembre 2015, n. 208 (di seguito legge di stabilità 2016), relativo ad una carta elettronica, utilizzabile per attività culturali, destinata ai giovani che compiono diciotto anni di età nell'anno 2016, formulando alcune osservazioni (provv. 28 luglio 2016, n. 328, doc. web n. 5387638).

In particolare, è stata riscontrata la mancata individuazione del ruolo assunto, nel trattamento dei dati personali, da parte dei diversi soggetti istituzionali coinvolti (Mibact, Presidenza del Consiglio dei ministri - Dipartimento per l'informazione e l'editoria, AgID, Sogei S.p.A. e Consap S.p.A.) e la mancata specificazione, delle modalità di realizzazione e gestione della piattaforma informatica dedicata, del tempo di conservazione dei dati personali, nonché delle misure di sicurezza predisposte. Si è ribadita, inoltre, la necessità di prevedere le eventuali comunicazioni di dati personali tra diversi titolari del trattamento con la specificazione che le finalità del trattamento dei dati siano limitate alla sola realizzazione dei compiti attinenti all'attribuzione e all'utilizzo della carta elettronica.

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 evidenzia il provvedimento recante l'Intesa sullo schema di linee guida Anac recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico (provv. 15 dicembre 2016, n. 521, doc. web n. 5860807).

In merito, si ricorda che la disciplina in materia di trasparenza contenuta nel d.lgs. 14 marzo 2013, n. 33, recante riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni è stata da ultimo modificata con l'approvazione del d.lgs. 25 maggio 2016, n. 97.

Al riguardo, è stata, fra l'altro, introdotta una nuovo tipologia di accesso civico – cd. generalizzato – in quanto è stato previsto che "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, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-*bis*" (art. 5, comma 2, d.lgs. n. 33/2013).

Il legislatore del 2016, nel disciplinare i casi di esclusione e i limiti al predetto accesso civico, ha previsto che "Ai fini della definizione delle esclusioni e dei limiti all'accesso civico […], l'Autorità nazionale anticorruzione, d'Intesa con il Garante per la protezione dei dati personali e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, adotta linee guida recanti indicazioni operative" (art. 5-*bis*, comma 2, d.lgs. n. 33/2013).

In tale quadro, l'Anac, ai sensi delle disposizioni richiamate, ha sottoposto al Garante uno schema di 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 (di seguito linee guida sull'accesso civico), sui cui l'Autorità è stata chiamata a esprimere l'Intesa.

Il testo iniziale dello schema di linee guida è stato elaborato anche nell'ambito di un apposito tavolo di lavoro, istituito presso l'Anac, cui ha partecipato il Garante fin dalla sua costituzione. Nel corso delle numerose riunioni, delle interlocuzioni, anche informali, e dei successivi approfondimenti sono state fornite indicazioni all'Anac volte a perfezionare il testo, per renderlo conforme alla disciplina in materia di protezione dei dati personali. Nel redigere lo schema di provvedimento sottoposto al Garante ai fini di acquisirne l'intesa, l'Anac ha valutato

anche le osservazioni pervenute durante la consultazione pubblica e i contributi istruttori acquisiti nel corso di audizioni informali cui è stato presente anche il Garante.

La versione finale delle linee guida sull'accesso civico ha, in linea di massima, recepito le indicazioni rese dall'Ufficio, anche se su alcuni punti il Garante, nel rendere l'Intesa, ha espresso alcune riserve. In primo luogo, con riferimento al par. 5.2, rubricato "Limiti (eccezioni relative o qualificate)", nella parte relativa alla valutazione sull'esistenza di un pregiudizio concreto che possa giustificare il diniego dell'istanza di accesso generalizzato, nell'Intesa è stato precisato che l'inciso contenuto nelle predette linee guida secondo il quale "L'amministrazione è tenuta quindi a privilegiare la scelta che, pur non oltrepassando i limiti di ciò che può essere ragionevolmente richiesto, sia la più favorevole al diritto di accesso del richiedente" non può essere interpretato nel senso di accordare una generale prevalenza al diritto di accesso generalizzato a scapito di altri diritti ugualmente riconosciuti dall'ordinamento (quali, ad es., quello alla riservatezza e alla protezione dei dati personali). Ciò perché, in tal modo, si vanificherebbe il necessario bilanciamento degli interessi in gioco che richiede un approccio equilibrato nella ponderazione dei diversi diritti coinvolti, tale da evitare che i diritti fondamentali di eventuali controinteressati possano essere gravemente pregiudicati dalla messa a disposizione a terzi – non adeguatamente ponderata – di dati, informazioni e documenti che li riguardano. A tale bilanciamento sono, peraltro, tenute le pp.aa nel dare applicazione alla disciplina in materia di accesso generalizzato, secondo quanto ribadito dalle stesse linee guida sull'accesso civico. In caso contrario, vi sarebbe il rischio di generare comportamenti irragionevoli in contrasto, per quanto attiene alla tutela della riservatezza e del diritto alla protezione dei dati personali, con la disciplina internazionale ed europea in materia (art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali; artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, direttiva 95/46/CE, regolamento (UE) 2016/679).

Analogamente, con riferimento al par. 6.3 delle citate linee guida, intitolato "Eccezioni assolute in caso in cui l'accesso è subordinato dalla "disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'art. 24 c. 1 della legge 241/1990", il Garante ha rilevato che a fronte delle indicazioni riportate nelle linee guida sull'accesso civico, si potrebbero generare dubbi interpretativi in ordine ai rapporti fra la disciplina sull'accesso agli atti, ai sensi della l. n. 241/1990, e quella dell'accesso civico "generalizzato", ai sensi del d.lgs. n. 33/2013. Tale problema deriva anche dalla formulazione testuale dell'art. 5-*bis*, comma 3, d.lgs. n. 33/2013, con riferimento all'individuazione delle eccezioni all'accesso civico nei casi di cui all'art. 24, comma 1, l. n. 241/1990 e dal rinvio, in esso contenuto, al regolamento del Governo di cui al comma 6, art. 24, l. n. 241/1990 e ai regolamenti delle singole amministrazioni. Sul punto, in assenza di un intervento chiarificatore del legislatore, il Garante ha auspicato che le predette incertezze possano essere superate, anche alla luce del monitoraggio sull'accesso, della prassi applicativa e della giurisprudenza che si formerà in materia, nell'ambito del previsto aggiornamento delle linee guida (cfr. 26.3).

4.3.2. Le pubblicazioni di dati personali online

In materia di diffusione di dati personali *online* per finalità di trasparenza o di pubblicità dell'azione amministrativa, il Garante è stato chiamato a pronunciarsi su numerose fattispecie nel dare riscontro a reclami, segnalazioni e quesiti, di cui si riportano solo i casi più rilevanti.

Nello specifico, si richiama ancora una volta il problema della diffusione *online* da parte di soggetti pubblici di dati sensibili, in quanto idonei a rivelare lo stato di salute dei soggetti interessati.

Il Garante ha, in proposito, censurato il comportamento di una Asl che aveva pubblicato *online* il testo integrale dell'allegato a un proprio decreto, il quale riportava in chiaro i dati personali (nome e cognome, data e luogo di nascita, indirizzo di residenza) dei soggetti assistiti che avevano fatto domanda per l'erogazione di contributi economici a favore di "pazienti affetti da particolari patologie che, malgrado, l'assistenza fornita dal Ssn, incorr[eva]no in rilevanti spese per ulteriori livelli di assistenza, anche di natura farmacologica" (provv. 10 marzo 2016, n. 106, doc. web n. 4916900 e 6 luglio 2016, n. 290, doc. web n. 5432325).

Analogamente il Garante è intervenuto nel caso della pubblicazione, da parte di una Asl sul proprio sito istituzionale, di documenti contenenti le proposte di liquidazione di rimborsi destinati agli assistiti dializzati, o per controlli *post* operatori, oppure assistiti in reparti Suap o *hospice* (dedicati come noto a soggetti che hanno subito gravi *deficit* neurologici dovuti a un danno delle strutture cerebrali oppure a malati terminali), con indicazione dei nominativi e codice fiscale dei soggetti interessati e in alcuni casi anche della data di nascita (provv. 17 marzo 2016, n. 125, doc. web n. 5045365 e 6 luglio 2016, n. 291, doc. web n. 5493629).

In un altro caso è stato stigmatizzato il comportamento di un comune che aveva pubblicato, sull'albo pretorio *online*, le determine con cui riconosceva il diritto di una propria dipendente, di usufruire dei permessi di cui alla l. n. 104 /1992 (legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate) per l'assistenza – rispettivamente – alla madre e al padre, riportando in chiaro, fra l'altro, i nominativi della menzionata dipendente e quelli dei relativi genitori, nonché la circostanza che questi ultimi erano portatori "di handicap grave", documentato da attestazione medica comprovante il relativo stato invalidante (provv. 21 luglio 2016, n. 316, doc. web n. 5440792).

In tutti i predetti casi è stato ricordato che "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 (artt. 22, comma 8, 65, comma 5 e 68, comma 3, del Codice. Cfr., inoltre, provv. 15 maggio 2014, n. 243, doc. web n. 3134436, recante linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, parte prima, par. 2 e par. 9.e.; parte seconda, par. 1; nonché i provvedimenti del Garante ivi citati in nota 49).

In merito è stato, altresì, evidenziato che anche la disciplina statale in materia di trasparenza prevede che "Restano fermi i limiti […] relativi alla diffusione dei dati idonei a rivelare lo stato di salute […]" (art. 7-*bis*, comma 6, d.lgs. 33/2013, che riproduce il testo dell'abrogato art. 4, comma 6), ed esclude – con riferimento agli "Obblighi di pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati" di importo superiore a mille euro erogati nell'anno solare – "la pubblicazione dei dati identificativi delle persone fisiche destinatarie dei [citati] provvedimenti, qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute […] degli interessati" (art. 26, comma 4).

È stata pertanto dichiarata l'illiceità del trattamento effettuato dagli enti sanitari e dal comune per aver diffuso *online* dati idonei a rivelare lo stato di salute, in vio-

lazione dell'art. 22, comma 8, del Codice. Inoltre, è stato ricordato che, in ogni caso, il trattamento dei dati personali deve avvenire nel rispetto del principio di necessità, pertinenza e non eccedenza (artt. 3, comma 1, e 11, comma 1, lett. *d*) del Codice), con la conseguenza che non risultava comunque giustificato diffondere, fra l'altro, dati quali l'indirizzo di abitazione o la residenza, oppure il codice fiscale (provv.ti 6 luglio 2016, nn. 290 e 291 doc. web nn. 5432325 e 5493629).

In tale quadro, è stato ritenuto, altresì, opportuno evidenziare che nei procedimenti di anonimizzazione dei documenti, la sostituzione del nome e del cognome dei soggetti interessati con le relative iniziali, può non essere una misura sufficiente a prevenire il potenziale rischio di re-identificazione dell'interessato, anche a posteriori, in particolari contesti o ambiti geografici, oppure mediante il collegamento con altre informazioni eventualmente nella disponibilità di terzi o ricavabili da altre fonti (provv. 6 luglio 2016, n. 290, cit. - cfr., in particolare nella parte prima, par. 3).

Più corretta è, invece, la sostituzione dei dati degli interessati con degli *omissis*, come era già stato fatto nello stesso decreto dell'Azienda sanitaria per gli altri dati personali, anche considerando che, nel caso di specie, la finalità di rendere pubblica la decisione dell'ente sanitario avente a oggetto rimborsi ai pazienti, poteva essere perseguita senza l'indicazione delle iniziali dei soggetti assistiti (artt. 3, comma 1, e 11, comma 1, lett. *d*), del Codice).

Sempre in tema di trasparenza, il Garante si è poi espresso in ordine alla pubblicazione *online*, sul portale di una regione, dei dati personali dei soggetti che avevano fatto domanda per ricevere contributi economici per interventi di risparmio energetico, ma la cui domanda non era stata accolta, oppure di soggetti che si trovavano in situazioni di disagio economico (provv. 18 maggio 2016, n. 228, doc. web n. 5385900).

Dall'accertamento effettuato era emerso, infatti, che dal sito web istituzionale della regione erano scaricabili e liberamente accessibili – con riferimento a un avviso pubblico per ottenere la concessione di contributi economici per interventi di risparmio energetico su unità abitative private – dati e informazioni personali (numero identificativo della domanda, nominativo del richiedente e, a seconda dei casi, comune dell'unità abitativa, costo preventivato complessivo, contributo concedibile oppure motivo dell'esclusione) contenuti in elenchi pubblicati a vario titolo e relativi a 10.019 persone. Per le istanze definite finanziabili, il contributo economico concedibile superava l'importo di mille euro, tuttavia di queste solo 935 (salvo scorrimento della graduatoria) sarebbero state finanziate, perché aventi la relativa copertura finanziaria.

Al riguardo, è stato ritenuto che le disposizioni dell'avviso pubblico regionale – non avendo natura di atto regolamentare (cfr. provv. 6 dicembre 2012, n. 384, doc. web n. 2223278) – non fossero idonee ai sensi dell'art. 19, comma 3, del Codice, per giustificare, anche in coerenza con quanto affermato nella sentenza della Corte costituzionale n. 271/2005, la pubblicazione dei nominativi di soggetti che avevano presentato l'istanza per la concessione del contributo economico e che si trovano in una situazione di disagio economico, oppure di soggetti la cui domanda era stata respinta o era ancora in fase istruttoria. Ciò perché, in caso contrario si sarebbe determinato un contrasto con le previsioni contenute nella disciplina statale in materia di trasparenza che – di contro – prevede la pubblicazione obbligatoria dei soli nominativi dei soggetti destinatari di un contributo di natura economica superiore ai mille euro, con esclusione – in ogni caso – della diffusione di dati identificativi delle persone destinatarie dei contributi da cui è possibile ricavare informazioni relative alla situazione di disagio economico (artt. 26 e 27, d.lgs. n. 33/2013).

Oltretutto, il citato avviso pubblico, prevedendo la possibilità di pubblicare dati e informazioni personali ulteriori rispetto agli obblighi di pubblicazione previsti da norme di legge o di regolamento, si poneva altresì in contrasto con l'art. 4, comma 3, d.lgs. n. 33/2013, che prevede tale facoltà solo "procedendo alla anonimizzazione dei dati personali eventualmente presenti". Pertanto, è stato vietato alla regione, ai sensi dei citati artt. 143, comma 1, lett. *c*), e 154, comma 1, lett. *d*), del Codice, di diffondere ulteriormente in internet, attraverso la pubblicazione nel sito istituzionale o sul bollettino ufficiale, i dati personali diversi da quelli indicati negli artt. 26 e 27, d.lgs. n. 33/2013, e precisamente quelli riferiti a soggetti che non risultano destinatari del contributo economico perché la relativa istanza è stata respinta o è ancora in fase istruttoria, nonché quelli riferiti a soggetti la cui collocazione in graduatoria poteva essere idonea a rivelare una situazione di disagio economico e quelli relativi alla procedura per il conferimento di contributi economici per interventi di risparmio energetico su unità abitative private. Contemporaneamente, è stato prescritto alla regione per il futuro, ai sensi degli artt. 143, comma 1, lett. *b*), e 154, comma 1, lett. *c*), del Codice – in assenza di una diversa norma di legge o di regolamento e al fine di provvedere ove necessario all'esigenza di far conoscere ai soggetti partecipanti le decisioni inerenti alle graduatorie di concessione di contributi economici per interventi di risparmio energetico su unità abitative private – di mettere a disposizione dei partecipanti alla procedura selettiva modalità di consultazione della collocazione in graduatoria mediante l'attribuzione agli stessi di credenziali di autenticazione (ad es., *username* o *password*, numero di protocollo, numero identificativo dell'istanza o altri estremi identificativi forniti dall'ente agli aventi diritto, oppure mediante utilizzo di dispositivi di autenticazione, quali la carta nazionale dei servizi) in aree ad accesso selezionato del sito istituzionale (cfr. provv. 15 maggio 2014, n. 243, cit., parte seconda, par. 3.b).

4.4. *La documentazione anagrafica e la materia elettorale*

In merito ad alcuni quesiti riguardanti le modalità di consultazione dei registri di stato civile per fini di ricerca storica, genealogica e di studio, è stato ribadito che la comunicazione di dati personali, da parte dei soggetti pubblici a privati, è ammessa unicamente quando è prevista da una norma di legge o di regolamento (art. 19, comma 3, e art. 11, comma 1, lett. *d*), del Codice), fatta salva la disciplina in materia di archivi pubblici storici (artt. 101-103, del Codice; codice di deontologia e buona condotta per i trattamenti di dati personali per scopi storici, All. A2, del Codice). Inoltre, con riferimento al peculiare regime di consultabilità degli atti e dei registri di stato civile (art. 450 c.c., artt. 106 e 107, d.P.R. n. 396/2000 e art. 177, del Codice), il Garante ha ritenuto condivisibili le indicazioni fornite al riguardo dal Ministero dell'interno – competente per materia – sull'accesso e la consultazione di tali atti da parte di soggetti privati che intendono effettuare ricerche di carattere storico, scientifico o statistico (cfr. Ministero dell'interno, massimario per l'ufficiale dello stato civile, 2012, par. 3.1.2) (nota 22 novembre 2016).

La Corte d'appello di Firenze ha formulato un quesito in tema di pubblicità delle dichiarazioni e dei rendiconti depositati dai candidati presso il Collegio regionale di garanzia elettorale (Corege) in relazione a due istanze pervenute, la prima da un'università, volta a consultare gli atti per una ricerca sulle varie forme di finanziamento nelle competizioni politiche e amministrative, e la seconda da un candidato (risultato non eletto) ad una competizione amministrativa, che ha chiesto di visionare gli atti, depositati presso il Corege, del competitore di un diverso schie-

ramento e risultato eletto. Al riguardo, l'art. 14, l. 10 dicembre 1993, n. 515, prevede che il Corege "riceve le dichiarazioni e i rendiconti di cui all'art. 7 e ne verifica la regolarità. Le dichiarazioni e i rendiconti depositati dai candidati sono liberamente consultabili presso gli uffici del Collegio". Tale documentazione riguarda: "la dichiarazione concernente le spese sostenute e le obbligazioni assunte per la propaganda elettorale" con "allegate le copie delle dichiarazioni (…) relative agli eventuali contributi ricevuti" (art. 2, comma 1, n. 3, della legge 5 luglio 1992, n. 441); –"un rendiconto relativo ai contributi e servizi ricevuti ed alle spese sostenute" nel quale sono "analiticamente riportati, attraverso l'indicazione nominativa (…) i contributi e servizi provenienti dalle persone fisiche" superiori a un determinato importo. Pertanto, richiamato il quadro normativo previsto per le comunicazioni di dati personali a soggetti privati –"anche mediante la loro messa a disposizione o consultazione" – l'Ufficio ha rappresentato che l'amministrazione interessata è tenuta semplicemente ad applicare, in modo corretto, la norma che rende ammissibile tale operazione (per es., con riferimento ai presupposti, ai limiti, soggettivi o temporali, alle finalità ed alle modalità previste per l'accesso) nel rispetto dei princìpi di pertinenza e di non eccedenza e, relativamente ai dati sensibili, del principio di indispensabilità (artt. 19, comma 3, 11, 20, 22, comma 3, e 65, del Codice). Fuori dai casi specifici previsti dalla normativa citata, ove ne ricorrano i presupposti, potrebbero trovare applicazione le norme generali in materia di accesso ai documenti amministrativi e di accesso civico (artt. 22 e ss. l. n. 241/1990; d.P.R. 12 aprile 2006, n. 184; artt. 59 e 60 del Codice; art. 5, d.lgs. n. 33/2013), con i limiti e le esclusioni previste dalle specifiche disposizioni (art. 24, l. n. 241/1990; art. 5-*bis*, commi 1, 2 e 3, d.lgs. n. 33/2013). Infine, con riferimento all'istanza formulata dall'università, è stato ricordato che per finalità di ricerca statistica e scientifica trovano applicazione le specifiche disposizioni previste dagli artt. 104 e ss., del Codice ed All. A. 4, codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (doc. web n. 1556635) (nota 11 ottobre 2016).

La Commissione di garanzia degli statuti e per la trasparenza e il controllo dei rendiconti dei partiti politici, ha richiesto un parere in merito alla possibilità di consentire la comunicazione di alcune informazioni contenute in documenti detenuti in base alle proprie prerogative istituzionali, ed in particolare l'esatto indirizzo della sede di un partito, il nome, cognome residenza e codice fiscale del legale rappresentante ai fini della tutela di pretese creditorie riconosciute con decreto ingiuntivo. La Commissione ha precisato che il partito del quale venivano richieste le informazioni non risultava iscritto nel registro nazionale introdotto dall'art. 4, d.l. n. 149/2013, convertito con l. n. 13/2014, e che, nella fattispecie, pertanto, non trovavano applicazione le prescrizioni che impongono la pubblicità dell'assetto organizzativo (statuto), comprensive dell'indirizzo e della sede legale, nonché dell'organo o del soggetto munito della rappresentanza legale. Al riguardo, è stato preliminarmente ricordato che, con riferimento a dati e informazioni concernenti persone giuridiche, enti o associazioni, non è applicabile la disciplina in materia di protezione dei dati personali (art. 40, comma 2, d.l. n. 201/2011, convertito con l. n. 214/2011). In merito ai dati delle persone fisiche, come i rappresentanti legali, sono state richiamate le norme che disciplinano la comunicazione di dati personali, comuni e sensibili, da parte dei soggetti pubblici (artt. 19, comma 3, e 20, del Codice), evidenziando che il Codice non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (artt. 59 e 60, del Codice; artt. 22 e ss., l. n. 241/1990; d.P.R. 12 aprile 2006, n. 184) (nota 9 agosto 2016).

4.5. *L'istruzione scolastica*

Nel settore scolastico il Garante ha interloquito sia con il Ministero dell'istruzione, dell'università e della ricerca (Miur), in relazione all'attività consultiva, che con singole università o istituti scolastici, nell'ambito di numerose istruttorie (n. 40).

In questo ambito un provvedimento di particolare rilievo è stato quello adottato il 21 aprile 2016 (n. 177, doc. web n. 5029548), con il quale il Garante ha espresso un parere sullo schema di decreto del Miur volto a disciplinare il periodo di conservazione di alcune tipologie di dati personali degli studenti, acquisiti all'Anagrafe nazionale degli studenti (Ans), di cui all'art. 3, d.lgs. 15 aprile 2005, n. 76 ed istituita presso il Miur con d.m. 5 agosto 2010, n. 74.

L'Ans contiene i dati sui percorsi scolastici, formativi e in apprendistato dei singoli studenti e i dati relativi alla loro valutazione, a partire dal primo anno della scuola primaria; essa si prefigge lo scopo di realizzare il diritto/dovere all'istruzione e alla formazione e per la prevenzione ed il contrasto alla dispersione scolastica (cfr. l'art. 3, d.lgs. n. 76/2005, cit.).

L'accesso all'Ans e all'omologa anagrafe degli studenti e dei laureati delle università, è esplicitamente disciplinato dalla legge che prevede che ad essa "accedono le regioni e gli enti locali ciascuno in relazione alle proprie competenze istituzionali. All'anagrafe degli studenti e dei laureati accedono anche le università […]" (art. 10, comma 8, d.l. 18 ottobre 2012, n. 179, convertito in l. 17 dicembre 2012, n. 221).

Lo schema di decreto esaminato dal Garante modifica il regime di conservazione dei dati personali acquisiti all'Ans, prevedendo la conservazione "perpetua" delle informazioni relative al "codice fiscale, codice della scuola che rilascia il titolo di studio, titolo di studio, voto conseguito, anno solare di conseguimento" (comma 2). La *ratio* del nuovo regime risiede nell'intento di "agevolare l'acquisizione e il controllo dei titoli di studio conseguiti dagli studenti da parte di altre pubbliche amministrazioni o enti tenuti per legge o regolamento ad acquisire d'ufficio tali informazioni" (cfr., il preambolo dello schema).

Al riguardo, l'Autorità ha rilevato, in primo luogo, che il testo della norma non permette di comprendere quali siano le ragioni che giustificherebbero l'allungamento del periodo di conservazione dei dati e ha quindi richiesto al Ministero di specificare più chiaramente le effettive finalità del trattamento, non solo per la valutazione della congruità del termine di conservazione, ma anche in relazione alla pertinenza e non eccedenza dei dati oggetto di conservazione. L'Autorità ha, inoltre, chiesto di individuare, con maggiore precisione, le informazioni a cui il decreto si riferisce e la disciplina del rispettivo periodo di conservazione (ferme restando le considerazioni che seguono in merito a quest'ultimo profilo), nel rispetto dei princìpi di finalità, necessità, pertinenza, non eccedenza e proporzionalità dei dati. La disciplina in materia di dati personali prevede infatti che la conservazione dei dati avvenga "in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati" (artt. 4, comma 1, lett. *a*), 11, comma 1, lett. *e*), del Codice). Tale principio è pertanto, in linea di massima, incompatibile con l'indicazione, riportata al comma 2 dello schema di decreto, che ipotizza una conservazione perpetua dei dati. Tale conservazione perpetua di dati personali porterebbe, in contrasto anche con la richiamata disciplina di settore, ad una duplicazione di dati, tenuto conto che le istituzioni scolastiche già sono obbligate – in virtù della disciplina in materia di conservazione dei beni culturali – alla conservazione perpetua dei propri documenti. Per tali ragioni l'Autorità ha condizionato il parere alla riformulazione dello schema di decreto con l'indicazione di uno specifico termine di con-

servazione dei dati, decorso il quale gli stessi devono essere cancellati o resi anonimi. L'Autorità ha infine rilevato che nel preambolo dello schema si legge che il Miur intenderebbe consentire alle università, nonché ad altre pp.aa. o enti tenuti per legge o regolamento ad acquisire d'ufficio tali informazioni, di accedere all'Ans per la verifica ed il controllo delle dichiarazioni sostitutive presentate dagli studenti in merito all'esito degli esami finali del secondo ciclo di istruzione e agli esami di qualifica. A tale proposito vale ricordare che, ai sensi della normativa in materia di certificati e dichiarazioni sostitutive, le amministrazioni pubbliche e i gestori di pubblici servizi sono tenuti ad acquisire d'ufficio le informazioni oggetto delle dichiarazioni sostitutive, nonché i dati e i documenti in possesso delle pp.aa. (cfr. l'art. 43, comma 1, d.P.R. 28 dicembre 2000, n. 445).

Al fine di agevolare l'accertamento di stati, qualità e fatti ovvero il controllo sulle dichiarazioni sostitutive presentate dai cittadini, le amministrazioni certificanti sono tenute a consentire, ai gestori di pubblico servizio o alle amministrazioni procedenti, la consultazione diretta per via telematica dei loro archivi informatici, nel rispetto della riservatezza dei dati personali e fermo restando il divieto di accesso a dati diversi da quelli di cui è necessario acquisire la certezza o verificare l'esattezza (cfr. l'art. 43, commi 2, 3 e 4, cit.).

Mentre l'accesso all'Ans da parte delle università per la verifica della veridicità dei titoli autocertificati è previsto da una specifica norma di legge (art. 5-*bis*, l. n. 264/1999), l'accesso da parte delle altre pp.aa. o enti, a cui si fa riferimento nel preambolo dello schema, tenuti ad effettuare d'ufficio il controllo dei titoli di studio autocertificati dagli studenti, non è stato ritenuto conforme al quadro normativo in quanto l'amministrazione o l'ente tenuto alla verifica dei titoli autodichiarati devono rivolgersi a questi fini direttamente alle amministrazioni certificanti che sono tenute alla conservazione del titolo oggetto di autocertificazione (nel caso di specie le singole istituzioni scolastiche presso le quali si è insediata la commissione esaminatrice che ha rilasciato il titolo). Su questo punto quindi il Garante ha condizionato il parere all'eliminazione dal provvedimento della possibilità di accesso all'Ans per le pp.aa. o per gli enti diversi dalle università per le finalità di controllo di cui sopra.

Il Miur ha presentato al Garante anche un altro schema di decreto per l'integrazione dell'Ans con ulteriori dati relativi agli alunni frequentanti le scuole dell'infanzia, sul quale il Garante si è espresso favorevolmente con provvedimento 12 maggio 2016 (n. 215, doc. web n. 5029436).

Con riguardo alle verifiche effettuate dall'Autorità in relazione a segnalazioni o reclami si evidenzia che in diversi casi (n. 5) essi hanno riguardato ipotesi di diffusione di dati personali di studenti su siti web (ad es., elenchi delle classi e dei diplomati con i loro numeri di telefono e quelli delle relative famiglie) o comunicazione di dati a soggetti esterni alle scuole (Asl o parrocchie) che sono risultate prive di idonee basi normative (note 10 febbraio e 4 aprile 2016).

Con riferimento alla diffusione dei dati tramite internet, inoltre, si registra in molti casi una non sempre oculata gestione dell'ambito di conoscibilità dei dati; nel contesto scolastico molte informazioni personali possono avere un ambito di circolazione che va oltre il diretto interessato e coinvolge anche la comunità scolastica (alunni, studenti, genitori, insegnanti) ma non possono invece essere diffuse sulla rete e rese disponibili a chiunque non faccia parte di detta comunità. In questo senso quindi il sito web può senz'altro facilitare forme di comunicazione sistematica mettendo a disposizioni taluni dati all'interno di un'area ad accesso riservato, ferma restando la riservatezza di informazioni di carattere personale che possono essere conosciute però solo dagli interessati e dalla loro famiglia.

Alcune gravi inosservanze discendono inoltre da una errata interpretazione degli obblighi di trasparenza ai quali sono tenuti gli istituti scolastici pubblici, come nel caso in cui un istituto statale ha effettuato una diffusione di dati personali, idonei a rivelare la vita sessuale di uno studente, in assenza di idonea base normativa (artt. 19, comma 3, e 20 del Codice; d.m. 7 dicembre 2006 n. 305). L'istituto infatti ha diffuso, sul proprio albo, anche *online*, ma prontamente rimosso a seguito dell'istruttoria, la delibera del Consiglio di istituto relativa alla sanzione disciplinare comminata a uno studente e recante informazioni legate, in senso lato, alla vita sessuale dello stesso (nota 15 novembre 2016).

In questi casi, oltre a rilevare l'illecito e a verificare che gli istituti coinvolti rimuovano dalla rete i dati illecitamente diffusi, viene avviato anche un procedimento sanzionatorio nei confronti dell'istituzione scolastica responsabile della violazione (art. 162, comma 2-*bis*, del Codice che prevede una pena pecuniaria da 10.000 a 120.000 euro).

Merita infine di essere citata la risposta a un quesito relativo alla possibilità, per gli alunni con una diagnosi di Dsa (Disturbi specifici dell'apprendimento), di fare uso, per fini personali, del registratore come strumento compensativo.

Al riguardo, è stato rilevato che la l. 8 ottobre 2010, n. 170, recante nuove norme in materia di disturbi specifici dell'apprendimento, prevede che gli studenti con tale patologia hanno diritto a fruire di appositi provvedimenti dispensativi e compensativi di flessibilità didattica. Su tali basi, le linee guida per il diritto allo studio degli alunni e degli studenti con Dsa precisano che gli interventi per l'esercizio del diritto allo studio di tali studenti si focalizzano, tra l'altro, proprio sull'uso di strumenti compensativi, ossia strumenti didattici e tecnologici che sostituiscono o facilitano la prestazione richiesta nell'abilità deficitaria. Tra queste, in un'elencazione non tassativa, le citate linee guida richiamano proprio "il registratore che consente all'alunno o allo studente di non scrivere gli appunti della lezione". Le attività di recupero individualizzato, le didattiche personalizzate e gli strumenti compensativi devono essere formalizzate nel piano didattico personalizzato dello studente condiviso con la famiglia dell'alunno.

Su tali basi è stato quindi ritenuto che nulla osti a che gli studenti con diagnosi Dsa possano utilizzare, senza l'acquisizione del consenso di soggetti terzi, gli strumenti compensativi di volta in volta previsti dalla scuola nei piani didattici personalizzati che li riguardano, ivi compreso il registratore (nota 18 marzo 2016).

4.6. *L'attività fiscale e tributaria*

Audit

Il Garante, nella riunione del 14 gennaio 2016, ha esaminato i primi esiti di un ciclo di accertamenti ispettivi volti a verificare l'osservanza delle norme in materia di protezione dei dati personali nelle procedure di registrazione degli accessi e di *audit* predisposte dalla Agenzia delle entrate e relativi all'Anagrafe tributaria. Tale attività si inserisce nell'ambito della vigilanza che il Garante esercita da anni sull'Anagrafe tributaria per la quale, negli anni 2015 e 2016, sono state programmate un complesso di verifiche funzionali ad accertare il rispetto delle specifiche prescrizioni impartite negli anni dall'Autorità, volte a prevenire accessi non autorizzati e trattamenti illeciti dei dati personali, nonché ad assicurare la qualità dei dati (pertinenza e non eccedenza, esattezza e aggiornamento).

Nell'ambito di questa attività sono emerse criticità riferibili ai sistemi di controllo sugli accessi e agli *alert* prodotti, dovute, in particolare, all'assenza di alcune tipologie di *alert* (interni, accessi contemporanei) e alla necessità di mettere a punto ade-

guate procedure di gestione e presa in carico degli stessi da parte dell'Agenzia e degli enti esterni. Per quanto riguarda, l'applicativo Fisconline e gli altri servizi *online* senza registrazione, sono state evidenziate criticità in relazione alle credenziali utilizzate e all'informativa fornita agli interessati. Le verifiche effettuate hanno anche messo in luce la necessità di attivare procedure di controllo sulla qualità dei dati; sono stati infatti rilevati errori negli importi riportati nell'applicativo dedicato al redditometro, riconducibili a difetti di comunicazione da parte dei soggetti obbligati, nonché nell'applicativo relativo al cd. spesometro, dove risultano importi di gran lunga inferiori a 3.600 euro (anche inferiori ai dieci euro) rispetto a quelli soggetti all'obbligo di comunicazione all'Agenzia delle entrate ai sensi dell'art. 21, d.l. n. 78/2010.

Le criticità rilevate, pur non costituendo in sé violazione di specifiche disposizioni o provvedimenti da parte dell'Agenzia, hanno comunque una specifica rilevanza in ragione della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità di realizzazione e gravità diverse per i diritti e le libertà degli interessati. Parte delle criticità rilevate sono state superate con l'adozione di tempestive misure correttive da parte dell'Agenzia e, dietro specifica richiesta dell'Autorità, con la predisposizione di un progetto organico per l'incremento dei livelli di sicurezza dell'Anagrafe tributaria comprensivo di una tempistica compatibile con la complessità tecnica dell'infrastruttura.

Dichiarazione dei redditi precompilata

Un altro rilevante tema di confronto con l'amministrazione finanziaria ha riguardato l'*iter* di approvazione della normativa di attuazione della cd. dichiarazione dei redditi precompilata.

In questo ambito il Garante, già nei pareri adottati nel 2015, aveva individuato specifiche misure a garanzia degli interessati tra cui, in particolare, le cautele per l'opposizione da parte dell'assistito all'invio dei dati relativi alle spese sanitarie al Mef per l'elaborazione della predetta dichiarazione, nonché le modalità di consultazione dei dati da parte dell'Agenzia e degli intermediari (pareri 30 luglio 2015, nn. 450 e 451, doc. web nn. 4160058 e 4160102) .

In coincidenza dell'approssimarsi della scadenze per l'invio dei dati al Sistema tessera sanitaria, istituito presso il Mef, da parte degli operatori sanitari per la dichiarazione precompilata 2016, a seguito della ricezione di numerosi quesiti da parte di medici in merito alla gestione dell'opposizione all'invio dei dati da parte degli assistiti, il Garante ha ritenuto necessario invitare il Ministero della salute, le regioni e provincie autonome, le principali associazioni operanti nel settore sanitario e in quello dei consumatori, a informare i propri iscritti e gli assistiti sulla possibilità di esercitare tale facoltà, senza che ciò determini il venir meno della possibilità di detrarre le spese sanitarie dal reddito, secondo le modalità ordinarie di compilazione della dichiarazione (nota 27 gennaio 2016, doc. web n. 4625287).

Al riguardo, il Garante è intervenuto anche sullo schema di provvedimento della Ragioneria dello Stato, volto a disciplinare le modalità di accesso alle spese sanitarie e relativa opposizione (provv. 4 febbraio 2016, n. 23, doc. web n. 4797834), nell'ambito del quale è stata data particolare attenzione al rispetto delle misure di sicurezza per l'accesso ai dati.

Il Garante si è espresso anche su quattro schemi di provvedimento del direttore dell'Agenzia delle entrate in relazione a nuovi flussi di dati per l'elaborazione della dichiarazione dei redditi precompilata, relativi alle spese funebri, alle spese universitarie, ai rimborsi delle spese sanitarie e contributi versati alle forme pensionistiche complementari di cui al d.lgs. 5 dicembre 2005, n. 252. (provv. 18 febbraio 2016, n. 63, doc. web n. 4716389).

Il Garante ha al riguardo indicato che occorre assicurare il rispetto del Codice, con particolare riferimento: a) alla pertinenza e non eccedenza dei dati raccolti, così

come indicati nei tracciati *record* (dati relativi alle spese sanitarie rimborsate, spese funebri); b) alla tutela dei diritti dei familiari a carico che non intendono far conoscere al soggetto dichiarante le proprie spese, in analogia a quanto disciplinato in materia di spese sanitarie, prevedendo anche per le spese universitarie la possibilità, per chiunque ne abbia interesse, di esercitare la propria opposizione all'inserimento di tali spese nella dichiarazione precompilata; c) alla corretta individuazione delle finalità del trattamento, evidenziando la necessità di specificare, negli schemi di provvedimento, che, oltre all'elaborazione della dichiarazione precompilata, i dati comunicati possono essere trattati anche per finalità di controllo sugli oneri deducibili e detraibili, anche ai sensi dell'art. 7, comma 5, d.P.R. n. 605/1973; d) alle misure di sicurezza, con particolare riferimento ai miglioramenti apportati al sistema Entratel.

Anche nel 2016 il Garante ha espresso il parere sul provvedimento del Direttore dell'Agenzia delle entrate avente per oggetto l'accesso alla dichiarazione 730 precompilata da parte del contribuente e degli altri soggetti autorizzati (parere 7 aprile 2016, n. 157, doc. web n. 4916838). Tale provvedimento, nell'ampliare la platea dei destinatari del 730 precompilato e delle informazioni destinate a confluirvi, tiene conto di alcune indicazioni fornite all'Agenzia delle entrate nell'apposito tavolo di lavoro, anche a seguito degli autonomi accertamenti effettuati dall'Autorità nei confronti dei Caf (cfr. par. 4.6). In particolare, sono state rafforzate le misure di sicurezza per limitare il rischio di accessi non autorizzati ai dati, migliorando il monitoraggio interno sulle operazioni effettuate dagli operatori abilitati. Sono stati altresì formulati cinque pareri in merito all'ampliamento dei dati da raccogliere per la dichiarazione precompilata 2017 (relativa all'anno di imposta 2016). In particolare, tali atti hanno disciplinato l'inclusione nella dichiarazione precompilata delle spese sanitarie sostenute presso i soggetti autorizzati, nonché di altre spese sanitarie (ovvero parafarmacie, psicologi, infermieri, ostetriche/i, tecnici sanitari di radiologia medica e ottici) e delle spese veterinarie (pareri 28 luglio 2016, n. 331, doc. web n. 5407377; n. 332, doc. web n. 5407413; n. 333, doc. web n. 5407516; n. 334, doc. web n. 5407586; n. 335, doc. web n. 5407732). In tale occasione è stato chiesto, in particolare, di espungere dagli atti esaminati le disposizioni che prevedevano l'utilizzo dei dati trasmessi al Sistema tessera sanitaria ai fini del cd. spesometro, che dovrà, invece, essere oggetto di ulteriori approfondimenti.

Nuove modalità di riscossione del canone RAI

Nel 2016, il Garante si è occupato della nuova modalità di riscossione del canone di abbonamento alle radioaudizioni (canone Rai) per i titolari di utenza elettrica, mediante addebito sulle fatture emesse a decorrere dal mese di luglio 2016.

La legge di stabilità 2016 (art. 1, commi 153 e ss., l. 28 dicembre 2015, n. 208) ha, infatti, introdotto una nuova disciplina fiscale basata sulla presunzione legale di possesso dell'apparecchio nel caso in cui esista un'utenza per la fornitura di energia elettrica nel luogo in cui un soggetto ha la sua residenza anagrafica. A tal fine, è stato stabilito che l'Anagrafe tributaria, l'Autorità per l'energia elettrica, il gas e il sistema idrico, l'Acquirente Unico S.p.A., il Ministero dell'interno, i comuni, nonché gli altri soggetti pubblici o privati che ne hanno la disponibilità, siano autorizzati allo scambio e all'utilizzo di tutte le informazioni utili, e, in particolare, dei dati relativi alle famiglie anagrafiche, alle utenze per la fornitura di energia elettrica, ai soggetti tenuti al pagamento del canone di abbonamento alla televisione, nonché ai soggetti beneficiari di agevolazioni.

Al riguardo, il Garante è intervenuto per i profili di competenza, in primo luogo, sullo schema di decreto attuativo del Ministero dello sviluppo economico, di concerto con il Ministro dell'economia e delle finanze, al fine di assicurare il rispetto del Codice (parere 27 aprile 2016, n. 192, doc. web n. 4943860).

4

Nel provvedimento il Garante ha rilevato criticità relative all'esatta individuazione del ruolo svolto dall'Agenzia delle entrate, dall'Acquirente Unico S.p.A. e dalle imprese elettriche nel trattamento dei dati dei soggetti obbligati al pagamento del canone e alla qualità dai dati personali utilizzati per individuare i soggetti a cui addebitare il canone in bolletta. Ha suscitato, infatti, perplessità la scelta di individuare i soggetti obbligati al pagamento del canone, automaticamente e in via presuntiva, attraverso i dati relativi alla tipologia di tariffa applicata per l'erogazione dell'energia D2 (clienti domestici con utenza nel luogo di residenza anagrafica), anche per i contratti stipulati antecedentemente al 2016, senza effettuare preventive verifiche con i dati di residenza presenti in anagrafe tributaria.

In relazione a ciò, pur valutando positivamente la capillare campagna informativa programmata e, in particolare, quanto prospettato dal Ministero dello sviluppo economico in relazione all'invio della comunicazione informativa ai titolari di contratti elettrici (per i quali l'addebito del canone sarebbe avvenuto solo a partire dalla fattura di luglio 2016), il Garante ha ritenuto necessario valutare separatamente la possibilità di ricorrere all'informativa semplificata ai sensi dell'art. 13, comma 3, del Codice, in modo da rendere pienamente conforme il trattamento alla disciplina di protezione dati.

Con provvedimento del 5 maggio 2016, il Garante ha, quindi, individuato le modalità semplificate con le quali le imprese elettriche, in fase di prima applicazione della nuova normativa, hanno dovuto integrare quella già fornita in sede di attivazione dell'utenza, circa l'utilizzo dei dati personali degli clienti anche per l'addebito del canone RAI. Tale informativa, resa attraverso un'apposita sezione dei siti web istituzionali delle imprese elettriche, dell'Agenzia delle entrate e della RAI, nonché nell'ambito del predetto piano informativo ministeriale, anche facendo rinvio al sito dedicato www.canone.rai.it e all'apposito numero verde, doveva specificare, in particolare, che i dati personali raccolti per la fornitura dell'energia elettrica sono utilizzati, in base alla tipologia di tariffa applicata (D2/D3), anche ai fini dell'individuazione dell'intestatario del canone di abbonamento e del relativo addebito in bolletta, che, in caso di tariffa D2 (tariffa residenti), avverrà in modo automatico (provv. 5 maggio 2016, n. 204, doc. web n. 5217043).

Infine, con provvedimento del 12 maggio 2016, nell'esprimere il parere sull'Intesa tra Agenzia delle entrate e Acquirente unico S.p.A. per la trasmissione dei dati utili all'addebito del canone tv nelle fatture per la fornitura di energia elettrica, l'Autorità ha prescritto l'adozione di specifiche misure di sicurezza per lo scambio di dati tra i predetti soggetti (provv. 12 maggio 2016, n. 216, doc. web n. 5217271). È stato, pertanto, prescritto all'Agenzia delle entrate e ad Acquirente unico di realizzare un collegamento sicuro con un sistema di *file transfer* sicuro (SFTP o FTP/S) oppure, in alternativa, un normale sistema FTP all'interno di un canale VPN IPsec o SSL, riducendo al minimo i rischi di violazione di dati personali contenuti nei sistemi informativi dei soggetti interagenti, con particolare riferimento a quello dell'Acquirente unico.

Attuazione della normativa FATCA

Nel 2016, il Garante è intervenuto nuovamente in merito all'attuazione della normativa FATCA (v. Relazione 2015, parr. 3.4.1., 4.6. e 22.3) da parte dell'Agenzia delle entrate, che ha sottoposto all'esame dell'Autorità due schemi di provvedimento (parere 6 luglio 2016, n. 289, doc. web n. 5387587).

Nel corso dell'istruttoria, sono state fornite indicazioni tecniche all'Agenzia delle entrate al fine di migliorare la sicurezza del trattamento dei dati personali, prevedendo come condizione la cifratura dei dati personali eventualmente oggetto di comunicazione agli operatori finanziari. Sono state, inoltre, richieste all'Agenzia specifiche garanzie in ordine al trattamento delle informazioni scambiate relative ai

rapporti finanziari degli interessati, e da sempre oggetto di particolari cautele nell'ambito della normativa di settore (cfr. ad es., cd. indagini bancarie, archivio dei rapporti finanziari, comunicazione integrativa annuale). Al riguardo, l'Agenzia ha assicurato che, non appena saranno definite delle politiche accertative che implicheranno l'utilizzo di questi dati e, quindi, le modalità e i soggetti autorizzati ad accedervi, ne sarà fatta comunicazione al Garante. Per quanto riguarda, invece, i dati raccolti e trasmessi in sede di prima applicazione della normativa FATCA, l'Agenzia ha dichiarato che i dati, conservati presso Sogei S.p.A., sono stati finora trattati esclusivamente in relazione alle operazioni strettamente necessarie all'adempimento connesso allo scambio automatico di informazioni.

Con riferimento ai trattamenti effettuati da Equitalia S.p.A. a fini di riscossione a mezzo ruolo, il Garante ha collaborato al fine di individuare garanzie per la protezione dei dati personali nell'ambito delle nuove iniziative intraprese per agevolare la comunicazione con i cittadini. In particolare, sono state fornite indicazioni per l'attivazione dei nuovi servizi di consultazione dell'estratto conto presso gli Atm e attraverso un'apposita applicazione, nonché per l'avvio, su richiesta di coloro che presentano un'istanza di rateazione *ex* art. 19, d.P.R. n. 602/1973, di un servizio che consenta agli interessati di ricevere, via sms o via *e-mail*, comunicazioni in merito all'eventuale rischio di decadenza dal piano di rateizzazione in caso di mancato pagamento delle relative rate, ovvero (ove il debitore lo desideri) anche altre informazioni riguardanti l'attività di riscossione di somme affidate in carico alla stessa Equitalia.

Trattamenti di dati relativi all'attività di riscossione

4.7. *La videosorveglianza in ambito pubblico*

Di particolare rilievo nel 2016 il settore dei trattamenti effettuati per mezzo di sistemi di videosorveglianza sia in ambito scolastico che sanitario-assistenziale. Diversi fatti di cronaca hanno alimentato infatti un vivace dibattito pubblico circa la possibilità di installare sistemi di videosorveglianza all'interno di asili o case di cura, al precipuo fine di prevenire atti di violenza nei confronti di minori o anziani.

La possibilità per gli asili e gli istituti di cura di utilizzare sistemi di videosorveglianza per tale scopo non è attualmente prevista e disciplinata dalla legge e, anche il provvedimento generale del Garante in materia (8 aprile 2010, doc. web n. 1712680*),* non prevede questa possibilità.

Al dibattito pubblico si è affiancato anche quello politico con la presentazione, in Parlamento, di alcuni disegni di legge volti a prevedere la possibilità di attivazione di tali sistemi; in questo contesto, l'Autorità ha offerto al legislatore il proprio contributo nell'ambito di due distinte audizioni (cfr. par. 3.1. in merito alle audizioni del Presidente presso le Commissioni riunite I e XI della Camera dei deputati del 27 luglio 2016 e presso la XI Commissione lavoro e previdenza sociale del Senato della Repubblica del 22 novembre 2016 (doc. web nn. 5301830 e 5696272).

In tale ultima audizione è stato sottolineato come "la liceità del fine perseguito non è di per sé sola sufficiente per legittimare l'uso generalizzato e continuativo di telecamere in strutture deputate alla relazione di cura e che ospitano soggetti la cui personalità, ancora *in fieri*, potrebbe essere segnata da esperienze di controllo sistematico (soprattutto i bambini potrebbero sviluppare una concezione "distorta" della propria libertà, considerando come appartenente alla "normalità" il fatto di essere sempre controllati)".

Proprio il carattere massivo di tali controlli, a prescindere da specifici indicatori di rischio e dal ricorso a mezzi meno invasivi, potrebbe risultare in contrasto con

quel principio di proporzionalità centrale nel formante giurisprudenziale europeo in materia di protezione dati.

È stato sottolineato infatti come l'invasività di tali forme di controllo – in un contesto, quale quello educativo, che più di ogni altro dovrebbe essere improntato a spontaneità e assenza di condizionamenti esterni – determini l'esigenza di uno scrutinio stringente sotto il profilo del rispetto dei princìpi di necessità e proporzionalità (cfr. in tal senso anche il parere 160/2009 del Gruppo Art. 29 sulla protezione dei dati personali dei minori, nonché il riscontro fornito dalla Commissione europea a un'interrogazione inerente il tema delle videocamere negli asili nido -P 6536-2009- che, nel qualificare – in linea generale – come legittimo l'interesse perseguito, ha tuttavia ribadito l'importanza del rispetto dei princìpi di necessità e proporzionalità del trattamento).

Ferma questa riserva di fondo, è stato altresì rappresentato che "l'ammissibilità dell'installazione delle telecamere soltanto in presenza di fattori di rischio specifici, previa individuazione dei soggetti deputati a valutarne la concreta sussistenza, potrebbe rendere la disciplina proposta più compatibile con il principio di proporzionalità e ragionevolezza cui deve attenersi ogni possibile bilanciamento tra diritti e libertà fondamentali".

Il tema dell'utilizzo di sistemi di videosorveglianza in ambito scolastico è stato trattato anche con riferimento alla possibilità di "autorizzare" l'installazione di *webcam* per consentire ai genitori dei bambini di una sezione della scuola dell'infanzia di collegarsi tramite *smartphone* per visualizzare le immagini dell'aula e la trasmissione in *streaming*, sul canale della scuola delle attività didattiche.

La peculiarità del contesto educativo e la possibile interferenza che l'utilizzo dei sistemi prospettati avrebbe potuto determinare nella relazione che caratterizza il fisiologico rapporto educativo proprio dell'istituzione scolastica, unitamente alle maggiori cautele e garanzie che devono essere rispettate nel trattamento dei dati dei minori (individuate anche dal Gruppo Art. 29 nel citato parere), hanno fatto ritenere che un tale trattamento di dati personali si ponesse in contrasto con i princìpi di necessità e proporzionalità (v. sul punto anche provv. 8 maggio 2013, doc. web n. 2433401).

Come già avvenuto negli ultimi anni, anche nel 2016, il Garante è stato più volte chiamato a esprimersi in ordine al trattamento di dati personali effettuato tramite sistemi di videosorveglianza in ambito pubblico.

Tra i molteplici chiarimenti forniti, si segnalano quelli relativi alla liceità del dispositivo denominato "fototrappola" (predisposto per rilevare delle immagini solo al verificarsi di certe condizioni predefinite), al fine di contrastare il fenomeno dell'abbandono incontrollato di rifiuti urbani. Al riguardo, è stato evidenziato che, qualora non risulti possibile, o si riveli inefficace, il ricorso a strumenti e sistemi di controllo alternativi, l'utilizzo di sistemi di videosorveglianza risulta lecito anche per accertare l'utilizzo abusivo di aree impiegate, come discariche di materiali e di sostanze pericolose e 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).

Sotto diverso profilo, invece, non risulta prevista dall'ordinamento vigente la possibilità di pubblicare le immagini, riprese attraverso i sistemi di videosorveglianza, di coloro che risultano aver violato le disposizioni sul conferimento di rifiuti. In diversi casi è stato evidenziato che, ove l'ente amministrativo ritenga utile, in un'ottica di sensibilizzazione, pubblicare *online* le immagini, delle persone che conferiscono in modo non conforme i rifiuti, rilevate dai predetti sistemi di video-

sorveglianza, è necessario considerare che il mero oscuramento del volto del soggetto interessato, in determinate circostanze e situazioni di contesto (ad es., sesso, conformazione fisica, fascia d'età, abbigliamento, strada ripresa, ecc.), potrebbe non rivelarsi uno strumento sufficiente a evitare il rischio di identificabilità degli interessati.

In un altro ambito, la presenza di un cartello riportante l'indicazione "Attenzione-Rilevazione automatica delle infrazioni con semaforo rosso" è stata ritenuta idonea a soddisfare, nello specifico contesto, il principio di trasparenza del trattamento dei dati previsto dall'art. 13 del Codice; ciò sulla base del principio, contenuto nel citato provvedimento generale in materia di videosorveglianza, in base al quale "l'obbligo di fornire tale informativa deve ritenersi soddisfatto anche quando il titolare del trattamento, pur mancando una previsione normativa che obblighi specificamente a segnalare la rilevazione automatizzata, la segnali comunque utilizzando avvisi analoghi a quelli previsti dal Codice della strada" (cfr. punto 5.3., provv. cit.).

Non è mancata occasione di pronunciarsi, anche in ambito sanitario, sul monitoraggio dei pazienti effettuato tramite sistemi di videosorveglianza nei locali del pronto soccorso, per specifiche esigenze di cura e tutela della salute. In tal caso, è stato chiarito che il consenso degli interessati può considerarsi manifestato nell'ambito del consenso al trattamento, acquisito ai sensi degli artt. 26 e 75 del Codice, per fini di prevenzione, diagnosi, cura e riabilitazione; ciò, a condizione che l'utilizzo di sistemi di videosorveglianza sia stato espressamente indicato, tra le modalità del trattamento, nell'informativa resa all'interessato (fatte salve le ipotesi di emergenza e tutela della salute e dell'incolumità fisica prevista dall'art. 82 del Codice) (nota 2 gennaio 2016).

È stata infine sottoposta al Garante una verifica preliminare circa il trattamento di dati personali effettuato, tramite un sistema di videosorveglianza cd. intelligente, da attivare presso gli accessi e le uscite di emergenza di un edificio che ospita la sede dell'amministrazione di un ente, per finalità di sicurezza e di tutela del patrimonio. Il sistema prospettato prevedeva l'attivazione delle telecamere in caso di "scavalco" dei tornelli collocati presso gli accessi e l'effrazione delle uscite di emergenza, rilevato da appositi sensori, alla quale seguiva la registrazione di un video dell'evento e la trasmissione di un segnale di allarme alla sala di controllo presente nell'edificio, presidiata 24 ore su 24 da personale specializzato e adeguatamente formato.

Esaminate le caratteristiche del sistema, il Garante ha ritenuto proporzionato (e quindi ammissibile) il trattamento dei dati personali, anche in considerazione delle assicurazioni fornite dal titolare del trattamento in ordine all'assenza di finalità di controllo a distanza dell'attività dei lavoratori e degli accorgimenti adottati in relazione all'adozione delle misure di sicurezza, all'informativa agli interessati e alla conservazione delle immagini registrate (provv. 10 novembre 2016, n. 475, doc. web n. 5796716).

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

Nel 2016 sono continuate a pervenire numerose segnalazioni da parte di cittadini e di associazioni di consumatori sul trattamento dei dati personali connesso alle modalità di controllo delle procedure di raccolta differenziata dei rifiuti urbani prescelte dai comuni. Ciò ha riguardato soprattutto le ispezioni, effettuate da operatori ambientali, del contenuto dei sacchetti dei rifiuti, al fine di identificare presunti trasgressori delle prescrizioni relative alla raccolta differenziata dei rifiuti urbani.

In tali occasioni è stato ribadito, come già evidenziato negli anni precedenti, che agli organi addetti al controllo è riconosciuta la possibilità di procedere a ispezioni

di cose e luoghi diversi dalla privata dimora per accertare le violazioni di rispettiva competenza (art. 13, l. 24 novembre 1981, n. 689), ma tale facoltà deve essere esercitata selettivamente, nei soli casi in cui il soggetto, che abbia conferito i rifiuti con modalità difformi da quelle consentite, non sia in altro modo identificabile. Risulterebbe, quindi, invasiva la pratica di ispezioni generalizzate, da parte del personale incaricato (quali agenti di polizia municipale e dipendenti di aziende municipalizzate), del contenuto dei sacchetti al fine di trovare elementi informativi in grado di identificare, presuntivamente, il conferente (cfr. punto 4. *d*), provv. 14 luglio 2005, doc. web n. 1149822; note 10 e 26 ottobre 2016).

La Città metropolitana di Roma capitale ha sottoposto all'Autorità un progetto sperimentale sulla fiscalità dell'auto finalizzato a contrastare il fenomeno della mancata copertura assicurativa contro la responsabilità civile e le sue conseguenze, non solo economiche e sociali (difficoltà di risarcimento alle vittime della strada, costi a carico della collettività), ma anche di evasione fiscale dell'imposta provinciale "sulle assicurazioni contro la responsabilità civile derivante dalla circolazione dei veicoli a motore […] dove hanno sede i pubblici registri automobilistici nei quali i veicoli sono iscritti" (art. 60, d.lgs. n. 446/1997; art. 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 progetto è finalizzato all'invio di una nota di cortesia per segnalare ai soggetti residenti nel proprio territorio, l'assenza della copertura assicurativa obbligatoria e le possibili conseguenze, sia sanzionatorie e di sequestro del veicolo (art. 193, d.lgs. n. 285/1992; art. 13, comma 3, l. 689/1981), sia economico sociali. La base di dati che si intende utilizzare per la selezione dei destinatari è costituita dal sistema informativo della motorizzazione civile, tramite collegamento informativo in dotazione alla Polizia locale della Città metropolitana, dalla quale è possibile estrarre le targhe dei veicoli privi di copertura assicurativa e dei relativi proprietari (artt. 225 e 226, d.lgs. n. 285/1992; artt. 3 e 8, d.P.R. n. 634/1994). Tali dati sarebbero stati poi verificati – in base ad un accordo di collaborazione con Automobile club d'Italia (Aci-Pra) – applicando una serie di criteri per individuare, con ragionevole ed elevata probabilità, tra i veicoli non assicurati, quelli circolanti.

L'istruttoria, non ancora conclusa, ha tenuto conto delle caratteristiche del fenomeno che, per rilevanza e diffusione, riguarda unitariamente l'intero territorio nazionale, nonché delle competenze assegnate alle città Metropolitane (subentrate alle province), del ruolo assegnato dalla legge a numerosi soggetti pubblici e privati per contrastare l'evasione dell'obbligo assicurativo. Si fa riferimento, in particolare, al processo di dematerializzazione dei contrassegni assicurativi e della loro sostituzione con sistemi elettronici e telematici, che vede coinvolti i Ministeri dello sviluppo economico, delle infrastrutture e dei trasporti, l'Ivass e l'Ania con l'istituzione della banca dati dei contrassegni assicurativi (cfr. decreto Ministero delle infrastrutture e dei trasporti 09.08.2013, n. 110; d.l. 24.1.2012, n. 1, convertito in l. 24 marzo 2012, n. 27; d.l. n. 179/2012, convertito in l. n. 221/2012) e relativamente al risarcimento delle vittime, il Fondo di garanzia per le vittime della strada amministrato dalla Consap sotto la vigilanza del Ministero dello sviluppo economico, e finanziato con i contributi annuali delle imprese di assicurazione, commisurato ai premi incassati (cfr. artt. 285 e ss., d.lgs. n. 209/2005, codice delle assicurazioni private).

La Regione Lombardia ha effettuato una comunicazione al Garante, ai sensi degli artt. 19, comma 2, e 39, del Codice, volta a consentire l'acquisizione dalle Aziende ospedaliere della Regione dei dati relativi ai bambini nati come secondogeniti, terzogeniti e oltre, al fine di realizzare un'iniziativa di "informazione diretta ai soggetti interessati" concernente alcune misure di sostegno alla maternità e alla natalità introdotte con la delibera della Giunta regionale n. 4152, dell'8 ottobre 2015,

e in particolare di un contributo economico *una tantum* a favore dei neonati, escluso il primogenito, residenti nel territorio lombardo. I dati da acquisire – generalità e residenza della madre, nome ed ordine di nascita del neonato – rientrano tra quelli contenuti nelle dichiarazioni di nascita rese dai genitori alla "direzione sanitaria dell'ospedale o della casa di cura in cui è avvenuta la nascita" (art. 30, comma 4, d.P.R. n. 396/2000). L'Autorità ha al riguardo ammesso l'attivazione del flusso dei dati necessari alla realizzazione dell'iniziativa – quelli acquisiti dalle dichiarazioni di nascita rese dai genitori ai cd. punti nascita – a condizione che tale comunicazione avvenga nel rispetto della normativa dettata a tutela dei minori nonché di quanto previsto dall'art. 30, comma 1, d.P.R. n. 396/2000, relativamente ai dati personali della madre che abbia dichiarato di non voler essere nominata (provv. 27 gennaio 2016, n. 22, doc. web n. 4806818).

È stato sottoposto alla valutazione dell'Ufficio il comportamento di un assessore alle politiche sociali di un comune che, in occasione di un'intervista, avrebbe rilasciato alcune informazioni su soggetti beneficiari di provvidenze economiche; ciò, con riferimento al contenuto di un articolo, pubblicato su una quotidiano locale, concernente la concessione di contributi economici a favore di soggetti che si impegnavano a rendere servizi utili alla comunità. L'articolo in questione relativo ad una delle famiglie beneficiarie, pur non riportando alcun dato identificativo degli interessati, indicava la nazionalità, la composizione della famiglia e la circostanza che un membro della stessa si era impegnato a svolgere un servizio di sorveglianza all'uscita della scuola. In merito, è stato ricordato che la normativa statale di settore in materia di trasparenza stabilisce l'obbligo di pubblicazione degli atti di concessione «delle sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese, e comunque di vantaggi economici di qualunque genere a persone ed enti pubblici e privati», per i quali, tuttavia, «È esclusa la pubblicazione dei dati identificativi delle persone fisiche destinatarie dei provvedimenti di cui al presente articolo, qualora da tali dati sia possibile ricavare informazioni relative»: «allo stato di salute» o «alla situazione di disagio economico-sociale degli interessati» (art. 26, commi 2 e 4, d.lgs. n. 33/2013). Per le ulteriori indicazioni e cautele da adottare in tale ambito, è stato fatto riferimento alle 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 del 15 maggio 2014 (doc. web n. 3134436) (nota 23 maggio 2016).

La Regione autonoma della Sardegna ha formulato un quesito in merito alla possibilità di consentire all'Associazione nazionale per la protezione degli animali che ne aveva fatto richiesta, l'accesso diretto alla banca dati regionale dell'anagrafe canina. Al riguardo, è stato preliminarmente richiamato il quadro normativo previsto per le comunicazioni di dati personali a soggetti privati –"anche mediante la loro messa a disposizione o consultazione" (artt. 3 e 11, comma 1, lett. *b*) e *d*), 19, comma 3 del Codice). Nel caso specifico, la l.r. n. 21, 18 maggio 1994, oltre a prevedere la tipologia di informazioni che devono essere registrate nell'anagrafe canina (art. 4), precisa che tali dati "sono comunicati alle associazioni protezionistiche che ne facciano richiesta" (art. 5, comma 5). Inoltre, in sede di attuazione della normativa nazionale e regionale, adottata con d.P.G.r. Sardegna 4 marzo 1999, n. 1 (regolamento di attuazione della l. 14 agosto 1991, n. 281 e della l.r. 18 maggio 1994, n. 21 e della l.r. 1° agosto 1996, n. 35 sulla prevenzione del randagismo) è stato ulteriormente specificato che "i registri dell'anagrafe canina devono essere tenuti nelle Asl di appartenenza e copia relativa deve essere fornita, con i conseguenti aggiornamenti, all'Assessorato dell'igiene, sanità e assistenza sociale e ad ogni comune interessato. Le associazioni di volontariato possono richiedere copia degli stessi" (art. 14, comma 4). Pertanto,

come in ogni altra ipotesi in cui una disposizione normativa preveda puntualmente la comunicazione di dati personali, l'Amministrazione è chiamata ad applicare la norma che rende ammissibile tale operazione (per es., con riferimento ai presupposti, ai limiti, soggettivi o temporali, alle finalità ed alle modalità previste) nel rispetto dei princìpi di pertinenza e di non eccedenza (artt. 11 e 19, comma 3, del Codice), valutando, nel caso specifico, se l'Associazione richiedente rientra tra i soggetti legittimati. In tal caso, è possibile prevedere forme di interrogazione o di accesso alla banca dati, in conformità a quanto previsto dal d.lgs. 7 marzo 2005, n. 82 (Cad), in merito alla disponibilità dei dati delle pubbliche amministrazioni (art. 50, del Cad), nel rispetto delle prescrizioni contenute nel provvedimento di questa Autorità del 2 luglio 2015 (doc. web n. 4129029) (nota 25 novembre 2016).

Un altro caso ha riguardato un comune ove, al termine del mandato, alcuni Consiglieri e il Sindaco hanno presentato un reclamo in merito al trattamento dei dati personali connessi alla gestione degli *account* di posta elettronica istituzionale loro assegnati dall'ente. Gli interessati avevano chiesto all'amministrazione comunale di poter accedere ai propri *account* e di estrarre una copia di tutti i *file* di posta elettronica contenuti nelle loro *mailbox*. La nuova giunta aveva stabilito, con delibera, che l'utilizzo delle caselle di posta assegnate, dichiarate risorse dell'amministrazione, cessa con il cessare della carica, disponendo la disattivazione delle *password* di accesso dei consiglieri uscenti e l'archiviazione del contenuto delle *mailbox* istituzionali del sindaco, assessore e consiglieri delle passate amministrazioni in un apposito *database* dedicato e protetto, anche per tenerli a disposizione dell'autorità giudiziaria per esigenze investigative connesse a una vicenda giudiziaria pendente presso la locale Procura della Repubblica. Nel caso di specie è stato rilevato che il comune non aveva reso ai reclamanti alcuna specifica informativa ai sensi dell'art. 13 del Codice in relazione al trattamento dei dati personali connessi alla gestione della posta elettronica né risultava adottato un disciplinare interno che regolasse l'uso delle risorse elettroniche dell'ente includendovi le informazioni obbligatorie indicate dall'art. 13 del Codice, così come previsto dal provvedimento in relazione al trattamento dei dati personali connessi alla gestione della posta elettronica (provv. 1 marzo 2007, n. 13, doc. web. 1387522) e ha invitato il comune ad adottare un disciplinare interno che regoli l'uso delle risorse elettroniche dell'ente, includendovi le informazioni obbligatorie indicate dall'art. 13 del Codice (nota 19 febbraio 2016).

In relazione alla segnalazione di un trattamento dei dati personali dei cittadini nell'ambito di una indagine conoscitiva, realizzata *online* utilizzando il servizio Google *forms*, erogato in modalità *cloud*, da parte di un comune, volto a rilevare le preferenze sulla chiusura o meno al traffico veicolare di una piazza, è stato rilevato che i dati raccolti (nome e cognome, età e indirizzo *e-mail*) erano stati conservati dal comune, nonostante il sondaggio fosse stato concluso e i tempi che ne giustificavano la conservazione ampiamente scaduti e che l'informativa, resa nell'ambito del sondaggio, non era conforme all'art. 13 del Codice. L'ente, a seguito dell'istruttoria, ha provveduto a cancellare i dati e, per i profili relativi all'informativa, è stato avviato un procedimento sanzionatorio (nota 19 febbraio 2016).

Osservatorio per il monitoraggio dei flussi di manodopera impiegata nella ricostruzione *post*-sisma in Abruzzo

Nel corso dell'anno, l'Autorità è stata investita anche delle problematiche legate ai trattamenti di dati personali necessari al monitoraggio dei flussi di manodopera impiegata nella ricostruzione *post*-sisma in Abbruzzo. In questo quadro, è stato innanzitutto consentito all'Inps di avvalersi del particolare regime previsto dagli artt. 19 e 39 del Codice per permettere all'Osservatorio per il monitoraggio dei flussi di manodopera, istituito presso la Prefettura de L'Aquila, di fruire di alcuni dati personali necessari allo svolgimento delle attività di prevenzione e controllo della mano-

dopera irregolare (cfr. art. 180, comma 2, d.lgs. 12 aprile 2006, n. 163; art. 16, comma 2, d.l. 28 aprile 2009, n. 39 convertito con modificazioni dalla l. 24 giugno 2009, n. 77; d.m. 14 marzo 2003; linee guida del Ministero dell'interno-Comitato di coordinamento per l'alta sorveglianza delle grandi opere del 30 ottobre 2014).

In particolare, non sono stati ravvisati ostacoli per la comunicazione alla Prefettura, da parte dell'Inps, di alcune informazioni estrapolate dalla banca dati Uniemens dell'Istituto riferite alle sole aziende, preventivamente individuate dalla stessa Prefettura, che operano in settori di attività collegati agli appalti, nonché ai relativi collaboratori e lavoratori. Ciò, in considerazione della natura dei dati personali oggetto di trasmissione, che non comprendono informazioni sensibili e giudiziarie, nonché della prospettata limitazione dell'ambito delle aziende interessate dal predetto flusso di informazioni, rispetto a quanto inizialmente rappresentato. Tali informazioni saranno quindi utilizzate dall'Osservatorio per ricavare "indicatori di incongruenze" relative alla disponibilità di manodopera tra le aziende coinvolte nella ricostruzione, consentendo così alla Prefettura di prevenire possibili flussi irregolari di manodopera e di indirizzare i necessari controlli sui cantieri, anche mediante la segnalazione di eventuali anomalie ai competenti organi di vigilanza. Al riguardo, l'Ufficio ha sottolineato il doveroso rispetto dell'obbligo di rendere l'informativa agli interessati "all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione" ai sensi dell'art. 13, comma 4, del Codice (nota 23 giugno 2016).

4.9. *La previdenza e l'assistenza sociale*

Attuazione del casellario dell'assistenza

Il Garante, con provvedimento del 28 luglio 2016, ha reso parere favorevole su uno schema di decreto direttoriale Inps riguardante le modalità attuative dei flussi informativi e disciplinare tecnico per la sicurezza, ai sensi del d.m. 16 dicembre 2014, n. 16 - casellario dell'assistenza - seconda e terza componente (n. 337, doc. web n. 5385436).

Il casellario dell'assistenza gestito dall'Inps è composto, oltre che dalla banca dati delle prestazioni sociali agevolate (già disciplinata dal decreto del Ministero del lavoro dell'8 marzo 2013 e dal decreto direttoriale dell'Inps n. 8 del 10 aprile 2015), dalla banca dati delle prestazioni sociali (che raccoglie le informazioni non incluse nella banca dati delle prestazioni sociali agevolate, nonché quelle sulle prestazioni di natura previdenziale erogate dall'Inps e sulle agevolazioni tributarie acquisite dall'Anagrafe tributaria rilevanti per il Sistema informativo dei servizi sociali - SISS), e dalla banca dati della valutazione multidimensionale per la presa in carico del beneficiario (organizzata in tre sezioni: Infanzia, adolescenza e famiglia attraverso il modulo SINBA - Sistema informativo sulla cura e la protezione dei bambini e delle loro famiglie; Disabilità e non autosufficienza attraverso il modulo SINA - Sistema informativo degli interventi per le persone non autosufficienti; Povertà, esclusione sociale e altre forme di disagio attraverso il modulo SIP -Sistema informativo su interventi e servizi sociali a contrasto della povertà e dell'esclusione sociale).

La delicatezza dei dati trattati, in particolare, nell'ambito della terza componente del casellario, e la complessità dei flussi informativi previsti dalle citate previsioni regolamentari, hanno imposto l'individuazione di misure e accorgimenti tecnici idonei a garantire elevati *standard* di sicurezza.

Lo schema di decreto direttoriale esaminato dal Garante è il frutto di un'intensa collaborazione con l'Inps e il Ministero del lavoro e delle politiche sociali, volta a definire le specifiche tecniche e le regole di sicurezza al fine di garantire un elevato

standard nei trattamenti delle informazioni contenute nelle banche dati delle prestazioni sociali e delle valutazioni multidimensionali, con riferimento ai flussi di dati trasmessi dagli enti erogatori e dall'Agenzia delle entrate. Sono state, inoltre, individuate specifiche cautele nell'individuazione delle tipologie di dati contenuti nel casellario da comunicare al Ministero del lavoro, alle regioni e alle province autonome, ai comuni e al Mef. Tali misure e accorgimenti sono individuati nel disciplinare tecnico allegato allo schema di decreto recante regole tecniche e di sicurezza per la trasmissione e la fruibilità delle informazioni della seconda e terza componente del casellario dell'assistenza (banca dati prestazioni sociali e banca dati delle valutazioni multidimensionali per la presa in carico).

In particolare, l'attenzione del Garante è stata rivolta ad assicurare che l'acquisizione dei dati attraverso il modulo SINBA, relativo ai minori, come previsto dalla normativa di settore, avvenga in forma individuale e priva di ogni riferimento che ne permetta il collegamento diretto con gli interessati nonché con modalità che, pur consentendo il collegamento nel tempo delle informazioni riferite ai medesimi individui, rendano questi ultimi non identificabili, garantendo la non reversibilità del processo di associazione tra le informazioni raccolte attraverso il modulo SINBA e le altre presenti nel casellario. Il disciplinare prevede, infatti, che gli enti erogatori, tramite un proprio apposito algoritmo di cifratura, creino un codice identificativo univoco per ciascun minore, beneficiario di prestazioni, avendo cura di utilizzare sempre lo stesso algoritmo per la generazione del codice, in modo da consentire al casellario il collegamento nel tempo delle informazioni riferite ai medesimi individui e da garantire al contempo che questi non siano direttamente identificabili. Il codice fiscale dei minori è utilizzato dagli enti erogatori solo in un primo momento, per acquisire dal casellario le informazioni sulle eventuali ulteriori prestazioni sociali o sulle prestazioni sociali agevolate di cui il minore è beneficiario, estraendole dal sistema informativo Isee, al fine di associarle a quelle da trasmettere all'Inps tramite il modulo SINBA. A seguito di tale operazione, gli enti trasmettono al casellario soltanto i dati, corredati del solo codice identificativo univoco dei beneficiari, cui sono stati applicati livelli di aggregazione tali da garantire la non identificabilità degli interessati, con la generalizzazione dei campi in cui le variabili risultano inferiori a cinque. A tale proposito, il disciplinare precisa anche che questi dati devono essere inviati al casellario parallelamente e separatamente dalle informazioni relative alle altre prestazioni sociali e che il codice identificativo univoco, utilizzato dagli enti erogatori per tali operazioni, non deve essere riconducibile ad alcun soggetto censito nelle banche dati dell'Inps, che non deve conoscere né la chiave né l'algoritmo utilizzati per la generazione del predetto codice.

Sono, poi, state oggetto di esame approfondito, e puntualmente individuate nel disciplinare, le tecniche di anonimizzazione finalizzate a rendere disponibili le informazioni contenute nel casellario, per l'alimentazione del SISS "in forma individuale ma prive di ogni riferimento che ne permetta il collegamento con gli interessati e comunque secondo modalità che rendono gli interessati non identificabili" al Ministero del lavoro e delle politiche sociali, a fini di monitoraggio della spesa sociale e valutazione dell'efficienza e dell'efficacia degli interventi, nonché per elaborazioni a fini statistici, di ricerca e di studio, e alle regioni e province autonome, ai comuni e agli altri enti pubblici responsabili della programmazione di prestazioni e di servizi sociali e socio-sanitari, con riferimento al proprio ambito territoriale di azione, per fini di programmazione delle prestazioni sociali, oltre che per le finalità di monitoraggio della spesa e valutazione degli interventi, nonché per scopi statistici, di ricerca e di studio.

Nell'ambito del disciplinare sono state altresì definite le modalità di aggregazione dei dati resi disponibili al Mef ai fini del monitoraggio della spesa sociale e per elaborazioni a fini statistici, di ricerca e di studio.

Nell'ambito della collaborazione istituzionale, è stato previsto, infine, un rafforzamento delle misure di sicurezza, prevedendo l'utilizzo di canali sicuri e di tecniche di cifratura per la trasmissione dei dati al casellario da parte degli enti erogatori, nonché il ricorso a un collegamento sicuro e alla cifratura dei dati per l'acquisizione delle informazioni sulle agevolazioni tributarie presso l'Agenzia delle entrate.

4.10. *L'attività giudiziaria*

Sicurezza nelle intercettazioni

Con provvedimento del 28 luglio 2016 (n. 336, doc. web n. 5385167) l'Autorità è nuovamente intervenuta sulla delicata materia delle misure di sicurezza nelle attività di intercettazione da parte delle procure della Repubblica con specifico riferimento alle prescrizioni oggetto del provvedimento del 18 luglio 2013 (n. 356, doc. web n. 2551507) e ha ulteriormente differito al 31 gennaio 2017 il termine per l'adempimento delle misure di sicurezza non ancora adempiute, già prorogato con provvedimento del 25 giugno 2015 (n. 375, doc. web n. 4120817).

In particolare, il Garante ha accolto la richiesta di differimento del predetto termine del Ministero della giustizia sulla base della documentazione trasmessa dal Ministero stesso e degli approfondimenti svolti in seno ad un tavolo di lavoro interistituzionale, nonché in considerazione delle prescrizioni impartite dall'Autorità con il menzionato provvedimento del 2013.

Pubblicazione di sentenze a fini di informazione giuridica

È proseguita in un clima di proficua collaborazione istituzionale l'attività di approfondimento con gli uffici della Corte di cassazione e con il Segretariato generale della giustizia amministrativa sul delicato tema della pubblicazione delle sentenze nei siti web istituzionali delle autorità giurisdizionali.

Nell'anno di riferimento, si registrano importanti pronunce della Corte di cassazione e del Consiglio di Stato in ordine alla pubblicazione in sentenza dei dati sanitari. In particolare, la Suprema Corte (Cass. civ., sez. I, 20 maggio 2016, n. 10510), dichiarando illecita la diffusione delle generalità del ricorrente tramite la pubblicazione nel sito della Corte dei conti di una sentenza (della medesima Corte), indicante lo stato di salute e le invalidità del ricorrente, ha osservato che "l'art. 22 Codice *Privacy* afferma il principio generale per cui i dati sensibilissimi, e specificamente quelli idonei a rivelare lo stato di salute, non possono essere diffusi. Tale indicazione, che non pare ammettere eccezioni, supera il punto di equilibrio indicato dall'art. 52, con riferimento ai provvedimenti giurisdizionali, tra gli interessi della persona alla *privacy*, di sicura rilevanza costituzionale, e quelli, altrettanto rilevanti, all'integrale pubblicazione dei provvedimenti giurisdizionali, a scopo di informativa giuridica".

Anche il Consiglio di Stato, nel rendere il parere sullo schema di decreto legislativo recante modifiche e integrazioni al codice dell'amministrazione digitale (C.d.S., affare n. 430/2016), oltre ai casi di oscuramento obbligatorio dei dati contenuti nei provvedimenti giurisdizionali previsti dall'art. 52, ha ravvisato "l'oscuramento obbligatorio dei dati concernenti la salute, ai sensi dell'art. 22, comma 8 […]".

Da segnalare altresì il riscontro fornito alla Camera arbitrale per i contratti pubblici, presso l'Anac, su un quesito che prospettava la pubblicazione, nel sito internet della stessa, del testo integrale dei lodi arbitrali depositati presso la Camera arbitrale (nota del Presidente 17 marzo 2016, doc. web n. 4965558). Al riguardo, considerato che le norme sulla protezione dei dati personali si applicano alle persone fisiche

e non alle persone giuridiche (art. 4, comma 1, lett. *i*), del Codice), si è lasciata impregiudicata ogni valutazione sull'eventuale rilievo di esigenze di riservatezza di queste ultime al di fuori dell'ambito di applicazione delle norme sulla protezione dati. La questione è stata esaminata alla luce di due princìpi fondamentali espressi nell'art. 8 della Convenzione EDU, quello di legalità e quello di proporzionalità, che impongono, rispettivamente, un'espressa previsione normativa che autorizzi l'ingerenza dell'autorità pubblica nella sfera privata e un giudizio di bilanciamento fra interessi contrapposti laddove il diritto alla tutela della sfera privata si scontri con altri diritti parimenti tutelati, nonché alla luce del diritto alla protezione dei dati personali, di cui all'art. 8 della Carta dei diritti fondamentali dell'Unione europea. In questa prospettiva, ricordato il recente orientamento della Suprema Corte, in base al quale l'attività degli arbitri rituali "ha natura giurisdizionale e sostitutiva della funzione del giudice ordinario" (Cass. sez. un., ord. n. 24153 del 25 ottobre 2013), si è osservato che tale funzione si svolge in forme per alcuni profili peculiari, poiché, ai sensi dell'art. 824-*bis* c.p.c., il lodo è efficace dalla data della sua ultima sottoscrizione, senza che sia necessario il deposito in cancelleria, laddove, invece, "la sentenza del giudice esiste giuridicamente e tutti ne hanno scienza legale con la pubblicazione, a cura del cancelliere"(Cass. civ. sez. un., n. 13794 del 1 agosto 2012) che dà atto del deposito (art. 133 c.p.c.). Il deposito del lodo è, invece, richiesto per l'esecuzione dall'art. 825 c.p.c, che richiama il secondo comma del citato art. 133 sui modi con i quali la cancelleria dà notizia della sentenza alle parti costituite, ma non il primo comma, in base al quale la sentenza "è resa pubblica" mediante il deposito. Si è così rilevato che la pubblicità non è elemento necessario della fattispecie e che anche per i lodi in materia di contratti pubblici di lavori, servizi e forniture (v. art. 241, comma 9, del codice dei contratti pubblici, d.lgs. 12 aprile 2006, n. 163) il deposito nella cancelleria del tribunale non è necessario. In mancanza di previsione normativa in tal senso, non presente neppure nel Codice, non si è quindi ravvisato alcun elemento utile ad attribuire al deposito del lodo presso la Camera arbitrale (considerando, tra l'altro, che quello presso la cancelleria del tribunale è solo eventuale) un'efficacia analoga a quella del deposito della sentenza previsto dal citato art. 133, comma 1, c.p.c., ai sensi del quale "la sentenza è resa pubblica mediante deposito nella cancelleria del giudice che l'ha pronunciata", né, del resto, si sono rinvenute opinioni o decisioni che consentano di ritenere che tra i princìpi del giusto processo *ex* art. 6 della Corte EDU quello della pubblicità sia inderogabilmente riferito anche al lodo. Sulla base delle suesposte considerazioni (fermo il regime di accessibilità degli atti per chi ne abbia interesse, come puntualmente richiesto dalla giurisprudenza amministrativa in materia) appare necessario chiedersi se drastiche decisioni in tema di pubblicità non rischino – anche a prescindere da ciò che attiene alle aspettative delle parti – di risultare in contrasto con il citato principio di proporzionalità di cui alle fonti dell'ordinamento comunitario ed interno che lo richiamano e ad esso si informano (alla luce dell'art. 8 della Corte EDU). In quest'ordine di idee si è ricordato come l'Autorità abbia segnalato anche per le sentenze di legittimità, pubbliche e con funzioni nomofilattiche, l'esigenza di bilanciare le finalità di promozione della conoscenza, da parte dei cittadini, delle decisioni della Corte di cassazione con quella di rispettare la sfera privata delle persone interessate, anche alla luce dei rischi connessi alla loro indiscriminata accessibilità via web, indicati dalla sentenza della CGUE del 13 maggio 2014, in C-131/12 (Google Spain), quali quelli di indicizzazione, decontestualizzazione, finanche alterazione dei dati stessi. Pertanto, riscontrandosi una specifica e puntuale disciplina legislativa del regime di formazione e pubblicità degli atti in parola, si è concluso che la finalità di informazione giuridica, sia attraverso la pubblicazione, nel sito internet dell'Anac, del testo

integrale dei lodi arbitrali, sia attraverso la consegna di copie dei medesimi a soggetti terzi, potrà legittimamente svolgersi, in applicazione del richiamato principio di proporzionalità, previo oscuramento dei dati che consentano di individuare le persone coinvolte, dovendosi considerare nel lodo arbitrale quali interessati - sotto questo profilo - tutti coloro i quali sono menzionati nel lodo e non solo coloro per i quali esso ha efficacia.

Pubblicità dei dati nei procedimenti di espropriazione forzata

Anche nel 2016 sono giunte all'Autorità segnalazioni riguardanti il regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata introdotto dalla riforma del processo esecutivo (d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, dalla l. 14 maggio 2005, n. 80), che prevede la pubblicazione in appositi siti internet di copia dell'ordinanza del giudice che dispone sulla vendita forzata e della relazione di stima dei beni da espropriare. Al riguardo, l'Autorità ha richiamato l'attenzione delle competenti autorità giudiziarie sulla necessità di rispettare la normativa in materia di protezione dei dati personali e le prescrizioni di cui agli artt. 174, comma 9, del Codice e 490, comma 3, c.p.c. al fine di assicurare la piena tutela dei diritti dei debitori sottoposti all'esecuzione, omettendo l'indicazione del debitore e di eventuali terzi estranei alla procedura dagli avvisi d'asta, estendendo tale omissione anche alla documentazione allegata ai predetti avvisi (v. al riguardo provv. 7 febbraio 2008, doc. web n. 1490838).

Produzione di documenti in giudizio

Con riferimento a segnalazioni relative a trattamenti di dati personali nel corso di procedimenti giudiziari, il Garante, nel ricordare che l'art. 24, comma 1, lett. *f*), del Codice consente il trattamento di dati personali senza consenso laddove indispensabile per far valere o difendere un diritto in sede giudiziaria, ha confermato che spetta al giudice adito, se ritualmente richiesto, la competenza a valutare la liceità del trattamento dei dati personali (art. 160, comma 6, del Codice) (in particolare note 20 maggio e 9 novembre 2016).

Notificazioni di atti giudiziari a soggetti estranei alle procedure

In un altro caso, invece, essendo stata interessata la Procura della Repubblica, l'Autorità ha rappresentato che l'impossibilità di interferire con l'attività dell'autorità giudiziaria, dotata di poteri di accertamento ben più incisivi di quelli spettanti al Garante, rende, nei fatti, inattuabili gli accertamenti da parte dell'Autorità, indispensabili per assumere le determinazioni di competenza. Del resto, le verifiche che spettano all'Autorità possono risultare condizionate anche all'esito dell'esposto, quanto meno in ordine all'accertamento dei fatti. Ove perdurasse l'interesse alle determinazioni dell'Autorità, si è chiesto pertanto all'interessato di dare notizia dell'esito del procedimento civile e della querela dallo stesso presentata, per consentire di valutare se residuino margini per le decisioni di competenza dell'Autorità medesima (nota 4 aprile 2016).

5 La sanità

5.1. *I trattamenti per fini di cura*

In ambito sanitario, l'Autorità ha fornito numerosi chiarimenti sia ai singoli cittadini, che alle Istituzioni operanti in materia.

Si segnala, in particolare, la partecipazione al tavolo di lavoro del Cantiere sanità digitale, organizzato dal Forum PA, con il contributo scientifico dell'Osservatorio innovazione digitale in sanità del Politecnico di Milano. Il tavolo, composto da rappresentanti delle amministrazioni centrali, delle regioni, delle aziende ospedaliere e di esperti del settore, ha effettuato una mappatura delle migliori esperienze in sanità digitale e si è posto l'obiettivo di individuare soluzioni in grado di facilitare la realizzazione delle iniziative di sanità digitale. Il contributo dell'Autorità è stato diretto ad evidenziare a tutti i rappresentanti delle Istituzioni pubbliche e private partecipanti come la corretta applicazione della disciplina sulla protezione dei dati sia necessaria al fine di garantire non solo la tutela della riservatezza e della dignità degli interessati, ma anche l'integrità, la correttezza e la fruibilità dei dati trattati ponendosi quale fattore decisivo per il successo nella realizzazione dei progetti di sanità digitale.

Merita ulteriormente segnalare l'intervento del Presidente dell'Autorità che ha rappresentato al Ministro della salute e al Presidente della Conferenza Stato-Regioni la necessità di definire, nelle opportune sedi ed eventualmente anche a livello normativo, un quadro omogeneo di regole con riferimento alla gestione della scheda sanitaria tenuta dai medici di medicina generale, il cui uso impatta su milioni di assistiti. Il Presidente ha evidenziato, altresì, che la mancanza di una disciplina unitaria, a livello nazionale, sulla tenuta delle predette schede sanitarie determina una rilevante disomogeneità a livello locale e presta il fianco a comportamenti che possono riflettersi anche molto negativamente sui diritti degli interessati, sotto diversi profili, tra i quali anche quelli relativi alle modalità della conservazione della scheda in occasione della cessazione dell'attività del medico (nota 28 luglio 2016).

In varie occasioni, nell'attività istruttoria, è stata sottoposta all'Autorità la questione della liceità dell'utilizzo delle immagini di minori all'interno di campagne mediatiche finalizzate alla raccolta di fondi a sostegno delle famiglie di bambini affetti da gravi patologie. Al riguardo, in applicazione dei princìpi sottesi alle specifiche disposizioni di settore che assicurano una tutela rafforzata ai minori al fine di non pregiudicarne l'armonico sviluppo della personalità (Carta di Treviso, codice di autoregolamentazione tv e minori, codice di deontologia medica, nuove linee guida della pubblicità sanitaria concernente i dispositivi medici), è stato evidenziato di porre particolare attenzione alla diffusione di tali immagini, al fine di evitare che, in nome di un sentimento pietoso, si arrivi ad un sensazionalismo che finisce per divenire sfruttamento della persona, spesso lesiva della dignità (nota 12 aprile 2016).

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

Continuano a pervenire numerose segnalazioni relative alla mancata acquisizione del consenso informato del paziente per il trattamento dei suoi dati personali per finalità di cura. Tra le criticità riscontrate nelle istruttorie avviate si evidenziano numerosi trattamenti privi dell'informativa agli interessati e modelli di acquisi-

zione del consenso eccessivamente generici in ordine alle principali caratteristiche del trattamento.

Tra i modelli di informativa esaminati molti sono risultati carenti con riferimento all'individuazione delle finalità del trattamento e ai diversi presupposti legittimanti lo stesso, rendendo di fatto incomprensibile all'interessato lo scopo della raccolta dei suoi dati sulla salute. Sebbene le aziende sanitarie oggetto di accertamenti istruttori abbiamo provveduto alla modifica dei modelli di informativa e consenso in uso con i pazienti, sono stati instaurati nei loro confronti specifici procedimenti sanzionatori.

In questo ambito, merita evidenziare la corrispondenza intercorsa tra il Presidente dell'Autorità e il Presidente della Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri (nota 17 maggio 2016). In tale occasione, l'Autorità ha infatti fornito chiarimenti sulle modalità di raccolta del consenso dell'interessato, sui presupposti legittimanti i trattamenti per fini amministrativi effettuati dai medici, sulle misure di sicurezza da adottare per il trattamento dei dati personali con strumenti informatici, sulla formazione del personale coinvolto nel processo di cura dell'interessato e sulle garanzie per il trasferimento dei dati all'estero. In particolare, è stato evidenziato che il Codice prevede un sistema di manifestazione della volontà dell'interessato fondato sul cd. *opt-in*: il consenso deve essere espresso, non potendo desumersi lo stesso da un comportamento concludente dell'interessato. Sono state poi evidenziate le semplificazioni previste dal Codice al settore sanitario con specifico riferimento alla possibilità di acquisire il consenso oralmente, purché vi sia una sua documentazione per iscritto.

Un aspetto particolare attiene all'invio dei dati personali dei soggetti che hanno usufruito di una prestazione sanitaria ai fini dell'elaborazione del modello 730. In merito è stato ricordato che tale comunicazione è espressamente prevista dalla normativa di settore e, trattandosi di un trattamento di dati per finalità amministrative in ambito pubblico (predisposizione da parte dell'amministrazione finanziaria di uno strumento per facilitare il cittadino negli adempimenti fiscali), il presupposto di liceità è da individuarsi, pertanto, nella norma di legge di riferimento e non nel consenso dell'interessato (come per i trattamenti per finalità di cura); il dissenso all'invio costituisce invece una modalità di opposizione, contemplata da tale quadro normativo (nota 17 maggio cit.).

5.1.2. Il Fascicolo sanitario elettronico (Fse)

Nel 2016 ha rappresentato per l'Autorità un impegno significativo la partecipazione ai lavori del tavolo tecnico di monitoraggio e indirizzo per l'attuazione delle disposizioni inerenti il Fascicolo sanitario elettronico (Fse), che vede la partecipazione del Ministero dell'economia e delle finanze, dell'AgID, del Cnr, del coordinamento regionale e dei rappresentanti di numerose regioni, sotto la direzione del Ministero della salute.

Obiettivo di tali lavori è quello di superare le difficoltà tecniche e giuridiche che ostacolano ancora l'attuazione, su tutto il territorio nazionale, del Fse. In tale contesto, il Garante ha fornito il proprio contributo favorendo il dialogo con gli enti e le amministrazioni coinvolte, al fine di giungere a soluzioni applicative efficienti e rispettose delle disposizioni in materia di protezione dei dati personali, attraverso numerosi chiarimenti sull'applicazione della disciplina di protezione dei dati personali ai trattamenti effettuati attraverso il Fse (nota 17 ottobre 2016).

In particolare, è stato chiarito che la normativa vigente prevede due fattispecie di consenso per il Fse: quello all'alimentazione e quello alla consultazione. Il consenso all'alimentazione è richiesto per inserire nel fascicolo i dati e i documenti relativi alle

prestazioni erogate all'interessato. In mancanza di tale consenso il Fse rimane vuoto e, quindi, non è accessibile né per finalità di cura, né per finalità di ricerca e di governo.

Il consenso alla consultazione è invece richiesto per rendere il Fse (alimentato sulla base del primo consenso) accessibile agli operatori sanitari che prenderanno in cura l'interessato. In mancanza di tale consenso, il Fse potrà essere utilizzato solo per fini di governo e di ricerca, nel rispetto dei limiti stabiliti dal quadro normativo vigente. Il consenso alla consultazione del Fse deve essere espresso *una tantum*, ovvero senza raccogliere tale manifestazione di volontà ad ogni accesso dell'interessato presso una struttura sanitaria.

È stato inoltre necessario fornire chiarimenti in ordine all'accesso al Fse in emergenza. Al riguardo, è stato ribadito che è necessario distinguere il caso in cui sia indispensabile accedere al Fse, in quanto sussiste un rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato, da quello in cui l'accesso sia necessario per la tutela della salute o dell'incolumità fisica di un terzo o della collettività. Nel primo caso, il consenso alla consultazione del Fse per finalità di cura legittimerà tutti i trattamenti di dati personali effettuati per finalità di cura, ivi compreso quello fatto in emergenza per la salvaguardia della vita dello stesso interessato. Nel secondo caso è necessario far riferimento a quanto previsto nell'art. 76 del Codice, secondo cui si può prescindere da un ulteriore e specifico consenso dell'interessato se l'accesso al Fse sia indispensabile per la tutela della salute o dell'incolumità fisica di un terzo (cfr. autorizzazione generale n. 2/2016, n. 524, doc. web. n. 5803257). Qualora il Fse dell'interessato sia stato lecitamente istituito sulla base del consenso alla consultazione per fini di cura, lo stesso potrà pertanto essere utilizzato, senza un ulteriore e specifico consenso, anche nel caso sia necessario per la tutela della salute o dell'incolumità fisica di un terzo o della collettività.

Con riferimento al diritto dell'interessato di conoscere gli accessi che sono stati eseguiti sul proprio Fse, è stato chiarito che a quest'ultimo devono essere fornite le seguenti informazioni: indicazione della struttura e del reparto che ha effettuato l'accesso, data e ora dello stesso, senza però riportare i dati personali dell'utente che ha materialmente effettuato l'accesso; quest'ultima informazione dovrà essere registrata nei *file* di *log*, ma resa disponibile solo sulla base di una ulteriore specifica richiesta. È stato poi evidenziato che la garanzia che al Fse possano accedere solo i medici curanti non deriva dal riconoscimento all'interessato del diritto di selezionare i professionisti sanitari o le categorie di professionisti che possono accedervi, bensì dalla disposizione secondo cui l'accesso al Fse, per finalità di cura, deve essere limitato ai soggetti "che prendono in cura l'interessato" (art. 12, commi 3 e 4, d.l. 18 ottobre 2012, n. 179, convertito in l. 17 dicembre 2012, n. 221). La logica, sottesa a tale scelta, risiede nella considerazione che l'interessato non può sapere, a priori, quali saranno i professionisti che lo prenderanno in cura.

Con riferimento poi al quadro giuridico in tema di Fse si evidenzia che, alla fine del 2016, è stato adottato un emendamento di modifica dell'art. 12, d.l. 18 ottobre 2012, n. 179, convertito in l. 17 dicembre 2012, n. 221 (art. 1, comma 382, legge di bilancio 2017).

I principali aspetti legati alla protezione dei dati personali connessi a tale novella riguardano la messa a disposizione nel Fse, entro il 30 aprile 2017, dei dati presenti nel sistema TS (tessera sanitaria) relativi alle "esenzioni dell'assistito, prescrizioni e prestazioni erogate di farmaceutica e specialistica a carico del Ssn, ai certificati di malattia telematici e alle prestazioni di assistenza protesica, termale e integrativa" (comma 15-*septies*, art. 12, d.l. 18 ottobre 2012, n. 179, convertito in l. 17 dicembre 2012, n. 221). Al riguardo, tale intervento normativo è volto a favorire l'imple-

mentazione del Fse con dati e documenti già presenti sulla relativa infrastruttura nazionale di supporto, ma non modifica le specifiche disposizioni normative che disciplinano i singoli flussi di dati e documenti nel sistema TS. A tali specifiche disposizioni normative, dunque, occorre far riferimento per individuare le finalità del trattamento e i soggetti destinatari dei suddetti dati e documenti. Con riferimento, ad es., ai certificati di malattia telematici, è stato osservato al tavolo di lavoro con la Ragioneria generale dello Stato e con il Ministero della salute che tali documenti contengono informazioni di tipo amministrativo e non clinico e, in quanto tali, potrebbero avere una loro utilità solo se inseriti nella parte del Fse a disposizione dell'assistito. Diversamente, soggetti quali le strutture sanitarie del Ssn che prenderanno nel tempo in cura l'interessato, il Ministero del lavoro, il Ministero della salute e le regioni verrebbero a conoscenza di informazioni che la disciplina di settore ha previsto siano invece conoscibili solo all'Inps e, entro certi limiti, al datore di lavoro dell'interessato. La necessità di assicurare che solo i soggetti previsti dalla legge accedano alle informazioni presenti nei certificati di malattia, trasmessi telematicamente, si rende ancor più evidente con riferimento ai certificati legati allo stato di gravidanza come, ad es., quello di interruzione della gravidanza (cfr. parere 4 giugno 2015, n. 334, doc. web n. 4130998).

Una specifica riflessione è stata richiesta poi con riferimento alla tipologia di dati e documenti che legittimamente sono conservati sul sistema TS, al fine di individuare quelli che possono essere resi disponibili al Fse. Tale riflessione deve prendere le mosse dalla consapevolezza che, ad es., tutti i dati delle ricette inviati telematicamente attraverso il Sistema pubblico di connettività (Spc) devono rispettare quanto previsto dal decreto del Mef 27 luglio 2005, secondo cui "al termine del trattamento dei *file* per i controlli formali, (ovvero di avvenuta ricezione da parte dei destinatari dei flussi) il Ministero dell'economia e delle finanze provvede alla cancellazione dei codici fiscali contenuti nei *file* delle ricette".

5.1.3. I dossier *sanitari*

Anche a seguito dell'adozione delle linee guida in materia di *dossier* sanitario, (provv. 4 giugno 2015, n. 331, doc. web n. 4084632) sono continuate a pervenire segnalazioni in ordine al mancato rispetto delle disposizioni a tutela dei dati personali nei trattamenti effettuati attraverso i *dossier* sanitari aziendali. In particolar modo, sono state svolte attività istruttorie in merito a presunti accessi abusivi al *dossier* sanitario di un paziente da parte di professionisti sanitari che non lo avevano in cura. In alcuni dei casi in esame, tale consultazione sarebbe stata possibile simulando un accesso in emergenza del paziente (note 23 febbraio, 13 ottobre e 10 novembre 2016).

In materia si evidenzia che nel 2016 è stata definita una significativa attività istruttoria nei confronti di un'Azienda ospedaliera avviata a seguito di una segnalazione nella quale si lamentava la possibilità di accesso, da parte di ogni medico dell'Azienda, ai dati personali di qualsiasi soggetto avesse usufruito di una prestazione sanitaria nella stessa, nonché l'assenza di informativa e di richiesta di consenso per tale trattamento di dati personali. A seguito delle verifiche ispettive effettuate, l'Azienda ha posto in essere una complessa attività, al fine di adeguare i trattamenti di dati personali alle prescrizioni del Codice, con particolare riferimento all'individuazione dei trattamenti autorizzati per singola struttura, alla designazione di tutto il personale dell'Azienda a responsabile/incaricato del trattamento e all'aggiornamento dei modelli di informativa e consenso al trattamento dei dati personali.

Pur prendendo atto degli adempimenti posti in essere spontaneamente dall'Azienda, il Garante ha prescritto di modificare i modelli di informativa e con-

senso in uso per i trattamenti di dati personali effettuati mediante il *dossier* sanitario e per i trattamenti dei dati personali effettuati per fini di cura e di mettere in atto specifici accorgimenti che consentano al personale amministrativo di accedere alle sole informazioni indispensabili per assolvere alle funzioni amministrative cui sono preposti. L'Azienda è stata richiamata inoltre a effettuare verifiche periodiche circa la sussistenza dei presupposti che hanno originato l'abilitazione degli incaricati, migliorando i sistemi di *audit log* adottati e provvedendo alla registrazione delle operazioni di consultazione dei dati trattati mediante il *dossier* (provv. 22 giugno 2016, n. 273, doc. web n. 5410033).

In materia, merita evidenziare anche il parere reso dal Garante alla Regione Lazio sullo schema tipo di regolamento aziendale sul trattamento dei dati nei processi di diagnosi e cura (parere 12 maggio 2016, n. 218, doc. web n. 5177496).

La predisposizione del predetto schema tipo ha avuto origine dallo studio promosso dal Policlinico Umberto I di Roma nell'adempiere alle prescrizioni dettate dall'Autorità con il provvedimento 18 dicembre 2014, n. 610 (doc. web n. 3725976). Trattasi di uno schema di regolamento aziendale, da divulgare a tutte le strutture sanitare regionali, che censisce le finalità istituzionali perseguite dalle aziende sanitarie e specifica per ogni finalità perseguita i dati personali indispensabili al suo perseguimento tenendo conto anche dei trattamenti effettuati per fini di ricerca scientifica e per fini amministrativi strettamente correlati alla cura.

L'Autorità ha fornito specifiche indicazioni in merito ad alcuni aspetti come, ad es., ai limiti per i trattamenti, a fini diagnostici e di cura, dei dati idonei a rivelare le opinioni politiche, l'adesione a partiti ovvero ad organizzazioni a carattere politico. Ha riconosciuto inoltre lo sforzo di censire tutte le professioni sanitarie operanti all'interno delle strutture sanitarie – anche di tipo universitario – individuando per ogni categoria i presupposti normativi del trattamento dei dati, le finalità perseguite e i processi di diagnosi e cura in cui tali soggetti sono coinvolti. Tale analisi rappresenta un presupposto metodologico idoneo ad una corretta attribuzione dei profili per l'accesso agli strumenti informatici – ivi compreso il *dossier* sanitario – in uso presso le strutture sanitarie. L'Autorità ha poi evidenziato che occorre prestare particolare attenzione alle figure professionali presenti nelle strutture universitarie (tirocinanti, specializzandi, dottorandi), ove le finalità di formazione e di assistenza si devono necessariamente integrare, e alle associazioni di volontariato che sempre più frequentemente operano in campo sanitario. Al riguardo, l'Autorità ha quindi rilevato come il percorso seguito dalla Regione nello schema di regolamento si muova nella direzione sempre auspicata dal Garante di contemperare l'efficacia dell'intervento diagnostico e terapeutico con la protezione dei dati, assicurando, in ogni caso, il rispetto del diritto alla salute e alla riservatezza e dignità dei pazienti, valori imprescindibili in ogni percorso che miri a salvaguardare la vita umana e auspica che tale atto sia al più presto adottato e diffuso tra le aziende sanitarie che fanno capo alla Regione Lazio, affinché si possa rafforzare il processo di adeguamento alla disciplina della protezione dei dati personali.

5.1.4. Referti e documentazione sanitaria

Nel 2016 sono continuate a pervenire numerose segnalazioni riguardanti la consegna di documentazione sanitaria (referti, cartelle cliniche, certificati medici) a soggetti diversi dall'interessato (n. 20).

In alcuni dei casi esaminati è stato accertato che l'avvenuta consegna all'interessato di referti contenenti informazioni sanitarie di terzi o di certificati relativi allo stato di salute di altri soggetti era stata conseguenza di errori umani. Le strutture sanitarie coinvolte, nei cui confronti è stato avviato un procedimento sanzionatorio,

hanno provveduto a modificare le procedure di consegna dei referti e della documentazione sanitaria, al fine di ridurre il rischio di errore umano e hanno avviato iniziative di formazione nei confronti del personale coinvolto in tali operazioni (note 9 maggio, 14 settembre e 21 settembre 2016).

In merito alle modalità di consegna dei referti sanitari, si evidenzia anche il caso di una provincia dell'Italia settentrionale ove era stato avviato un servizio di consegna dei referti presso le erboristerie e parafarmacie locali: in questa circostanza si è invitato il titolare del trattamento al rispetto di quanto previsto dal quadro normativo vigente, secondo cui i referti relativi a prestazioni di assistenza specialistica ambulatoriale possono essere consegnati, oltre che presso la struttura sanitaria che li ha redatti, solo presso "farmacie pubbliche e private operanti in convenzione con il Servizio Sanitario Nazionale" (decreto Ministero della salute, 8 luglio 2011) e non anche per altre categorie di soggetti (nota 17 marzo 2016).

5.1.5. La tutela della dignità della persona

Una particolare attenzione hanno avuto le segnalazioni relative alla presunta violazione delle disposizioni dettate dal Codice e da specifiche disposizioni di settore a tutela della dignità delle persone in relazione al trattamento dei loro dati personali per finalità di cura (artt. 2 e 83, Codice; provv. 9 novembre 2005, doc. web n. 1191411).

In tale ambito, specifico interesse è stato prestato al trattamento dei dati personali delle donne che decidono di partorire in anonimato, con riferimento alla tutela della loro dignità e riservatezza (art. 30, comma 1, d.P.R. n. 396/2000). L'attività ha riguardato in particolar modo le richieste di soggetti – nati da donne che al momento del parto si sono avvalse del diritto di non essere nominate – di accedere alla documentazione sanitaria relativa alla propria madre biologica per motivi di tutela della salute. In tali casi, è stato ricordato che la tutela della riservatezza dell'identità delle madri, che al momento del parto si sono avvalse del diritto di non essere nominate, è attualmente prevista dal combinato disposto dell'art. 28, comma 7, l. n. 184/1983 (così come modificato dall'art. 177, comma 2, del Codice) e dall'art. 30, comma 1, d.P.R. n. 396/2000. A tali disposizioni si aggiunge la previsione del Codice secondo cui non possono essere resi noti, se non decorsi cento anni dalla formazione del documento, il certificato di assistenza al parto o la cartella clinica, a meno che in essi non vengano oscurati i dati personali che rendono identificabile la madre naturale che abbia esercitato il diritto a non essere nominata (art. 93). Al riguardo, è stato pertanto evidenziato che, come rappresentato dal presidente Soro nella lettera al Presidente della Commissione giustizia della Camera (segnalazione 25 settembre 2014), la sentenza della Corte costituzionale 18 novembre 2013, n. 278, evidenziata dagli interessati a sostegno delle loro richieste di accesso, non ha scalfito il diritto alla riservatezza delle madri che al momento del parto si sono avvalse del diritto di non essere nominate, non avendo la pronuncia interessato il menzionato art. 30, d.P.R. n. 396/2000. Al contrario, la Corte ha ribadito la necessità di cautelare in termini rigorosi il diritto all'anonimato delle donne "attraverso un procedimento, stabilito dalla legge, che assicuri la massima riservatezza" delle stesse. Nelle more della conclusione dell'*iter* legislativo in atto, è stato pertanto evidenziato che permane la vigenza della disciplina sopra richiamata relativa al diritto alla riservatezza delle madri che al momento del parto si sono avvalse del diritto di non essere nominate (nota 9 maggio 2016) (cfr. par. 22.4).

Nel 2016 è proseguito il controllo sull'attività svolta dalle Asl con riferimento alla somministrazione e distribuzione dei presidi sanitari. In particolare, in una fattispecie esaminata, è stata ritenuta illegittima la comunicazione di dati personali dei pazienti del servizio incontinenza effettuata da una Asl alla società che si era aggiu-

dicata la gara di appalto per la distribuzione degli ausili medici correlati a tale patologia. L'illiceità è stata riscontrata con riferimento al fatto che la suddetta società, pur effettuando un trattamento dei dati personali dei pazienti della Asl – contrariamente a quanto previsto nel capitolato tecnico regionale – non era stata designata responsabile del trattamento (nota 29 febbraio 2016).

In un altro caso, è stata avviata un'attività istruttoria a seguito di una segnalazione di un paziente che lamentava la presenza, sui pacchi contenenti presidi sanitari, di loghi e diciture che rendevano facilmente comprensibile che gli stessi contenessero prodotti per la gestione dell'incontinenza. Al riguardo, è stato ritenuto che l'insieme delle informazioni presenti sulla parte esterna dei pacchi destinati all'interessato (ad es., marchio del prodotto e taglia) fosse idoneo a rivelarne il contenuto, anche in considerazione del fatto che il marchio utilizzato è direttamente e comunemente collegato a una serie di prodotti dedicati alla gestione dell'incontinenza maschile e femminile. L'Asl per la quale avveniva la suddetta distribuzione ha provveduto a disporre una revisione delle regole per il trasporto e l'imballaggio dei prodotti, al fine di garantire che non ne venisse identificato il contenuto (nota 10 agosto 2016; cfr. provv. 21 novembre 2013, n. 520, doc. web n. 2803050). In entrambi i casi sopra riportati sono stati anche avviati specifici procedimenti sanzionatori.

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

Anche nel 2016 sono pervenute segnalazioni in merito al mancato rispetto delle misure a tutela della dignità e della riservatezza dei malati di HIV in occasione dell'erogazione di prestazioni sanitarie.

In questo ambito, merita evidenziare un caso in cui un'agenzia formativa ha chiesto di essere autorizzata a sollecitare, attraverso i competenti servizi sociali, la famiglia di una minorenne a sottoporre quest'ultima agli esami volti ad accertare l'eventuale presenza dell'infezione da HIV. Tale richiesta era motivata dalla circostanza che si riteneva necessario valutare il rischio di contaminazione biologica di un docente intervenuto in un incidente verificatosi nel centro di formazione professionale frequentato dalla minorenne.

Al riguardo, è stato rappresentato che la l. 5 giugno 1990, n. 135 (programma di interventi urgenti per la prevenzione e la lotta contro l'Aids) ha previsto che nessuno possa "essere sottoposto, senza il suo consenso, ad analisi tendenti ad accertare l'infezione da HIV se non per motivi di necessità clinica nel suo interesse" (art. 5, comma 3, della predetta legge). Alla luce di quanto sopra, considerato che le finalità di prevenzione, diagnosi e cura esulano sicuramente dalle competenze dell'agenzia formativa, si è ritenuto che qualunque suggerimento alla famiglia della minore, volto a sottoporla ad accertamenti nel senso indicato, sia del tutto inopportuno e comunque rimesso direttamente agli organismi sanitari ai quali competono le valutazioni e le iniziative più appropriate da adottare in questi casi (nota 12 aprile 2016).

Si evidenzia infine che, anche nel 2016, vi sono stati diversi casi in cui studi medici e strutture sanitarie sono state richiamate al rispetto del provvedimento 12 novembre 2009 (doc. web n. 1686068) in cui sono individuate specifiche garanzie per la raccolta d'informazioni sullo stato di sieropositività dei pazienti da parte degli esercenti le professioni sanitarie nello svolgimento delle proprie attività professionali. Con tale provvedimento il Garante ha vietato agli esercenti le professioni sanitarie di raccogliere l'informazione circa l'eventuale stato di sieropositività in fase di accettazione di ogni paziente che si rivolge a questi per la prima volta, indi-

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

5.2. *I trattamenti di dati sulla salute per fini amministrativi*

Anche nell'anno di riferimento sono state ricevute segnalazioni e reclami in ordine al trattamento dei dati personali effettuato per finalità amministrative correlate alla cura.

Un'articolata attività istruttoria ha riguardato alcune segnalazioni relative all'avvenuta comunicazione di dati sulla salute di numerosi pazienti e di dipendenti a regioni o altre amministrazioni pubbliche da parte di strutture sanitarie private accreditate per rappresentare, a tali enti, le particolari condizioni in cui versano (anche in termini di richiesta di prestazioni sanitarie) e per richiedere un aumento delle somme stanziate dai fondi regionali. In tali casi, il Garante ha rappresentato che le predette finalità potevano essere utilmente raggiunte anche senza indicare i nominativi e senza riportare le informazioni sanitarie sugli assistiti e sui dipendenti e ha, quindi, considerato la comunicazione di tali dati priva di idonea base normativa avviando specifici procedimenti sanzionatori (note 4 e 14 aprile 2016, 10 maggio 2016).

In un altro contesto, una regione è stata invitata a riformulare un progetto di prevenzione del tumore al seno che inizialmente prevedeva una raccolta generalizzata, da parte degli uffici amministrativi regionali, dei referti degli esami mammografici effettuati da tutte le donne residenti nel territorio, al fine di garantire una più efficace campagna di prevenzione. L'intervento ha consentito di realizzare comunque la pregevole iniziativa di *screening*, evitando una raccolta generalizzata di dati sanitari da parte di strutture amministrative non deputate alla cura della salute (nota 26 luglio 2016).

Analogamente, una azienda sanitaria ha modificato un progetto, in fase di realizzazione, volto ad instaurare un servizio di prenotazione di visite ed esami diagnostici tramite WhatsApp, sia per le criticità evidenziate in ordine al rispetto dei presupposti di liceità del trattamento e delle misure di sicurezza, sia perché scollegato rispetto alle modalità, anche digitali, offerte dal legislatore nazionale in materia di prenotazione delle prestazioni sanitarie da erogare a carico del Ssn (sistema Cup - linee guida nazionali del Ministero della salute d. m. 8 luglio 2011, sul quale l'Autorità ha fornito il proprio parere - provv. 19 gennaio 2011, doc. web n. 1787887). In questo caso, previo coinvolgimento anche del Ministero della salute, è stato evidenziato che il coordinamento, a livello centrale, delle modalità di erogazione attraverso strumenti digitali dei servizi sanitari del Ssn, consente di assicurare un livello uniforme di garanzie anche dal punto di vista della protezione dei dati personali (nota 26 luglio 2016).

I Centri unici di prenotazione

Tra i trattamenti di dati sulla salute per fini amministrativi correlati alla cura, particolare attenzione è stata prestata nei confronti delle attività effettuate dai Centri unici di prenotazione (Cup) delle aziende sanitarie.

Gli accertamenti svolti hanno riguardato in particolare la designazione a incaricati del trattamento del personale che opera nei Cup, il ruolo delle società che forniscono i relativi servizi alle aziende sanitarie, l'informativa da rendere agli interessati e la qualità e quantità dei dati nel sistema di prenotazione.

Merita evidenziare quanto emerso a seguito di una segnalazione relativa a un sistema Cup del centro Italia offerto da una società privata alle farmacie pubbliche e private abilitate al servizio di prenotazione delle prestazioni sanitarie erogate

dall'Asl locale. Il servizio di prenotazione telefonica veniva erogato attraverso il personale della società, operante esclusivamente presso le sedi societarie site anche all'estero, sulla base di designazioni a incaricato del trattamento effettuate direttamente dalle predette farmacie. Tale procedura è stata oggetto di rilievo in quanto di fatto tale personale non era sottoposto, come espressamente previsto dall'art. 30 del Codice, alla "diretta autorità" del titolare o del responsabile del trattamento, non avendo né la Asl né le farmacie interessate la effettiva possibilità di effettuare controlli puntuali e diretti nei loro confronti.

È stato altresì rilevato che la società esterna, che gestiva il servizio di prenotazione telefonica, offriva agli utenti anche un servizio di prenotazione per alcune strutture sanitarie private senza che l'azienda sanitaria ne fosse a conoscenza. L'operatore del Cup, nel caso in cui la prestazione richiesta dall'utente non fosse stata disponibile presso la Asl, o per la stessa fossero previsti tempi di attesa troppo lunghi, proponeva all'interessato di prenotare la medesima prestazione presso strutture sanitarie private. Tale condotta è stata ritenuta illegittima perché configurava, in assenza di alcun presupposto legittimante, un trattamento dei dati dei soggetti che si rivolgevano al Cup per finalità ulteriori rispetto alla prenotazione di prestazioni sanitarie presso le strutture del Ssn. Al riguardo, è stato quindi avviato un procedimento sanzionatorio (nota 10 novembre 2016).

In alcuni dei casi esaminati è stato rilevato che le aziende sanitarie non fornivano agli interessati una idonea informativa, ovvero procedevano alla richiesta di consenso al trattamento, effettuato nell'ambito della prenotazione richiesta, tramite i sistemi Cup. Al riguardo, è stato ricordato che il trattamento dei dati personali effettuato nell'ambito del sistema Cup si configura come un trattamento svolto per finalità amministrative, correlate all'attività di diagnosi e cura per il quale, fornita un'idonea informativa, non è richiesto il consenso dell'interessato. Il presupposto di liceità di tale trattamento, come di tutti quelli effettuati per finalità amministrative correlate alla cura, deve essere, infatti, rinvenuto nel rispetto del regolamento per i trattamenti dei dati sensibili e giudiziari delle aziende sanitarie adottato dalla regione di appartenenza (nota 3 ottobre 2016).

Con riferimento alla quantità e qualità dei dati e alla presenza dei dati storici nel sistema Cup, sono emerse notevoli criticità in merito alla tipologia dei dati consultabili dagli operatori relativi alle prestazioni sanitarie già erogate all'utente sia in regime di libera professione, sia a carico del Ssn. Le istruttorie effettuate hanno consentito di rivedere tali impostazioni riducendo al minimo indispensabile le informazioni disponibili, rendendo non più visualizzabili le prestazioni sanitarie già erogate all'interessato, in quanto la conoscenza di tali informazioni non è stata considerata, dalle stesse aziende sanitarie, necessaria all'operatore Cup per procedere all'attività di prenotazione richiesta (nota 30 marzo 2016).

Trasmissione dei dati nel Nsis

Riguardo al trattamento dei dati nell'ambito del Nuovo sistema informativo sanitario (Nsis), il Garante ha reso il parere (provv. 10 marzo 2016, n. 108, doc. web n. 4943801, cfr. par. 3.3.1) sull'aggiornamento del protocollo riguardante la trasmissione dei dati rilevati dalle ricette mediche, nell'ambito del Sistema tessera sanitaria, dal Mef al Ministero della salute, alle regioni e all'Aifa (Agenzia italiana del farmaco), ai sensi dell'art. 50, comma 10, d.l. 30 settembre 2003, n. 269, convertito, con modificazioni, dalla l. 24 novembre 2003, n. 326, e s.m.i.

L'aggiornamento trae origine dall'esigenza di rivedere il protocollo vigente (protocollo 9 marzo 2006, sul quale il Garante ha reso parere il 21 luglio 2005, doc. web n. 1151167) in ragione delle modifiche normative che hanno previsto nuovi flussi di dati tra i medici prescrittori e il Mef (comma 5-*bis* dell'art. 50 cit., come modificato dall'art. 1, comma 810, lett. *c*), l. 27 dicembre 2006, n. 296), la demateria-

lizzazione della ricetta medica cartacea (artt. 11, comma 16, d.l. n. 78/2010, d.m. 2 novembre 2011 e art. 13 d.l. 18 ottobre 2012, n. 179), nonché le disposizioni di attuazione dell'interconnessione dei sistemi informativi del Ssn, di prossima adozione. Ciò, in vista del rafforzamento degli interventi in tema di monitoraggio della spesa pubblica del settore sanitario, delle iniziative per la realizzazione di misure di appropriatezza delle prescrizioni, nonché dell'accelerazione del conseguimento dei risparmi derivanti dall'adozione di modalità telematiche per la trasmissione delle ricette mediche.

Al riguardo, si ricorda che la normativa sul Sistema tessera sanitaria prevede che i dati delle ricette mediche prescritte ed erogate, acquisiti telematicamente dal Mef, siano inseriti, con modalità esclusivamente automatiche, in archivi distinti e non interconnessi, uno per ogni regione, in modo che sia assolutamente separato quello relativo al codice fiscale dell'assistito.

Innanzitutto, con riferimento al richiamo, operato dal protocollo, a una serie di decreti ministeriali adottati in assenza del prescritto parere del Garante (tra i quali il decreto Mef 2 novembre 2011 sul Sistema di accoglienza centrale-Sac), l'Autorità ha segnalato di non poter esprimere in tale sede alcuna valutazione di competenza. Salva ogni valutazione su profili più prettamente procedurali, il parere è stato, quindi, reso sul presupposto che la disciplina del decreto ministeriale sul Sac sia conforme alla normativa in materia di protezione dei dati personali e di tutela della riservatezza.

Analogamente, poiché non è stato ancora adottato il regolamento di attuazione sulle procedure per l'interconnessione dei sistemi informativi nell'ambito del Nsis (art. 15, comma 25-*bis*, d.l. 6 luglio 2012, n. 95, convertito, con modificazioni, dalla l. 7 agosto 2012, n. 135), è stato rilevato che il parere dell'Autorità deve intendersi reso sul presupposto che il regolamento sarà adottato in conformità al parere del Garante del 9 marzo 2015 (doc. web n. 3869889).

Nel merito, in attuazione dei princìpi di pertinenza, non eccedenza e indispensabilità dei dati trattati, il Garante ha chiesto di indicare espressamente il sottoinsieme di dati che si prevede di trasmettere all'Aifa, al Ministero della salute e alle regioni tenendo presente che possono essere oggetto di trasmissione soltanto quelli strettamente necessari al perseguimento delle specifiche finalità istituzionali dei diversi enti destinatari (ad es., alle regioni vanno inviati esclusivamente i dati riferiti all'ambito territoriale di competenza).

È stata poi segnalata una disparità nel livello delle garanzie di riservatezza previste per i soggetti assicurati da istituzioni estere rispetto a quelli iscritti al Ssn. Tale disparità trae origine, in particolare, dal decreto 18 marzo 2008 che prevede che il codice personale e il codice della tessera sanitaria dell'assicurato da istituzioni estere, riportato sulle ricette, vengano inviati al Mef in chiaro, a differenza del codice fiscale dell'assistito dal Ssn che viene sottoposto ad un'operazione di cifratura. È stato quindi richiesto di applicare le medesime garanzie di riservatezza anche per i soggetti assicurati da istituzioni estere.

Altre osservazioni hanno riguardato il rispetto del principio di minimizzazione dei dati, con particolare riferimento alle previsioni del protocollo che includono, tra i dati oggetto di trasmissione all'Aifa, al Ministero della salute e alle regioni, quelli relativi alla provincia di residenza degli iscritti al Ssn, nonché i dati identificativi del medico prescrittore. Riguardo a questi ultimi, non è stata ritenuta adeguatamente giustificata la necessità del loro trattamento, alla luce delle finalità istituzionali perseguite dai predetti soggetti, destinatari dei dati, in capo ai quali, in base al quadro normativo di riferimento, non emerge, tra l'altro, alcun compito di controllo puntuale, neanche in forza delle nuove disposizioni sulla verifica dell'appropriatezza pre-

5

scrittiva del singolo medico (v. art. 9-*quater*, commi 4 ss., d.l. 19 giugno 2015, n. 78 conv. dalla l. 6 agosto 2015, n. 125 e d.m. 9 dicembre 2015). Sono stati quindi richiesti specifici accorgimenti volti a sostituire il codice identificativo del medico prescrittore con un codice univoco a livello nazionale che non consenta di identificare l'interessato (riguardo ad un analoga problematica cfr. parere del Garante 26 marzo 2015, n. 178, su uno schema di decreto ministeriale in materia di disciplina del flusso informativo sui dimessi dagli istituti di ricovero pubblici e privati, doc. web n. 3878687).

Con riferimento alla sicurezza dei dati, è stata segnalata la necessità di integrare il disciplinare tecnico del protocollo con l'indicazione delle misure adottate a tal fine, dei tempi di conservazione dei dati, trascorsi i quali questi devono essere cancellati o resi anonimi, nonché con opportune previsioni sui *file* di *log*, che devono registrare le operazioni di accesso ai sistemi ai fini della verifica della liceità del trattamento dei dati.

In via generale, è stato osservato come sia ormai superata e non adeguata alla particolare delicatezza dei dati trattati l'autenticazione degli utenti del Sistema tessera sanitaria tramite nome utente e *password*, prevista per la fase di prima attuazione del protocollo, anche in considerazione dell'evoluzione tecnologica e dell'imminente disponibilità del sistema Spid in conformità all'art. 64 del Cad.

6 I dati genetici

Cessione a terzi di una banca dati genetica della popolazione sarda

È da tempo all'attenzione del Garante la vicenda relativa alla cessione a terzi di una banca dati genetica della popolazione sarda, a seguito del fallimento della società di ricerca che la gestiva (v. Relazione 2014, p. 71 e Relazione 2015, p. 80). La banca dati contiene i campioni biologici di circa 12.000 individui insieme ai dati demografici, clinici, genetici e genealogici riguardanti rapporti di parentela risalenti fino al 1600.

Come si ricorderà, sulla base degli approfondimenti avviati nei riguardi del curatore fallimentare negli anni precedenti, nell'ambito delle attività prodromiche alla cessione a terzi della banca dati, l'Ufficio aveva raccomandato il rispetto della disciplina sulla protezione dei dati personali per i casi di cessazione del trattamento, specie con riferimento all'osservanza del principio di finalità e delle altre disposizioni il cui mancato rispetto avrebbe determinato l'inefficacia dell'atto di trasferimento e l'inutilizzabilità dei dati trasferiti (v. artt. 11, 16, 99 e 162, comma 1, del Codice).

Gli accertamenti dell'Ufficio erano poi proseguiti, anche *in loco*, a seguito delle notizie di stampa riguardanti l'avvenuta aggiudicazione della banca dati, all'esito della procedura fallimentare, a una società di ricerca con sede a Londra. Da tali accertamenti, è emerso che quest'ultima aveva costituito in Italia un'altra società, con l'intento di conferirle il patrimonio aziendale acquisito, comprensivo della biobanca, di proseguire il progetto di ricerca avviato dalla fallita e di svolgere ulteriori e diverse attività di ricerca nel campo del genoma umano, della diagnosi di malattie e dello sviluppo di nuovi farmaci mediante la medicina personalizzata.

Nel frattempo, altre notizie di stampa riportavano l'ammanco di 14.000 campioni biologici dalla sede del Parco genetico dell'Ogliastra, a Perdasdefogu, consorzio che aveva collaborato a suo tempo alle attività di ricerca, fornendo alcuni servizi (tra i quali la raccolta dei dati dei donatori, il prelievo dei campioni di sangue, l'estrazione del dna e la conservazione dei campioni biologici presso il laboratorio di Perdasdefogu). Al riguardo, l'Ufficio ha chiesto alla Procura della Repubblica di Lanusei, che stava indagando sulla vicenda, di mettere a disposizione dell'Autorità elementi utili alla valutazione del caso, per i profili di competenza, manifestando al contempo la propria disponibilità a fornire ogni chiarimento in merito (nota 12 settembre 2016).

Inoltre, un centinaio di donatori nel 2016 si sono rivolti all'Autorità, lamentando una serie di aspetti relativi al trattamento dei dati, effettuato a suo tempo nell'ambito della ricerca, tra i quali, l'incompletezza dell'informativa resa agli interessati, l'indebita raccolta dagli archivi anagrafici comunali dei dati volti a ricostruire gli alberi genealogici della popolazione, la carenza di misure di sicurezza adeguate, nonché l'impossibilità ad oggi di esercitare i loro diritti riguardo al trattamento dei dati e dei campioni contenuti nella banca dati a causa della mancanza di indicazioni utili a identificare con certezza l'effettivo titolare del trattamento.

Sotto altro profilo, gli accertamenti effettuati dall'Ufficio hanno consentito di riscontrare che la società londinese, aggiudicataria della banca dati, aveva già posto in essere le operazioni necessarie per l'esercizio delle attività di ricerca

scientifica (acquisizione e allestimento dei locali, reperimento di personale specializzato, etc.) ed era stata immessa nel possesso di parte dell'archivio cartaceo della fallita e dei supporti elettronici sui cui era memorizzata la banca dati. La stessa società, tuttavia, non aveva ancora la possibilità di accedere alle informazioni contenute nella banca dati, poiché ancora in corso le operazioni necessarie al ripristino della sua operatività, né aveva la disponibilità dei campioni biologici prelevati nel corso della ricerca, posti sotto sequestro dalla Procura della Repubblica di Lanusei nell'ambito delle indagini riguardanti la sottrazione dei campioni biologici dal laboratorio di Perdasdefogu.

Nel merito, l'Autorità ha ritenuto che l'avvenuta cessione della biobanca a un'altra società non aveva esaurito i suoi effetti sul piano civilistico, ma aveva investito anche l'aspetto relativo alla protezione dei dati personali delle persone che, fino a quel momento, avevano avuto contatti soltanto con la società, in seguito fallita, e con l'istituto di ricerca del Cnr, insieme al quale, quest'ultima aveva condotto, fino alla dichiarazione di fallimento, le attività di ricerca scientifica in Ogliastra. A seguito della cessione, conseguente al fallimento, infatti, la nuova società che ha acquisito la banca dati, non è solo subentrata in tutti i rapporti giuridici facenti capo alla fallita, ma ha anche assunto la qualità di titolare del trattamento dei dati e dei campioni ivi contenuti, necessitando quindi di un valido presupposto giuridico legittimante il trattamento.

In conformità a quanto prevede la disciplina sulla protezione dei dati personali in relazione all'utilizzo dei dati sensibili e genetici per scopi di ricerca scientifica (artt. 23, 90 e 107 del Codice e autorizzazione generale n. 8, punto 3, lett. *c*), anche alla luce del tenore dell'informativa resa a suo tempo ai donatori e delle dichiarazioni di consenso raccolte da questi ultimi, tale presupposto è rinvenibile nell'acquisizione di un nuova manifestazione di consenso degli interessati, preceduta da un'idonea formativa. Ciò, con riferimento, perlomeno, all'avvenuto mutamento nella qualità del titolare del trattamento dei dati personali e dei campioni biologici contenuti nella biobanca, nonché degli eventuali ulteriori trattamenti che il nuovo titolare ha dichiarato di voler effettuare per eseguire altre attività di ricerca in campo medico-genetico.

Sulla base delle risultanze degli accertamenti effettuati dall'Ufficio, la società cessionaria della banca dati, non è tuttavia risultata, allo stato, in possesso di tali necessari presupposti.

Pertanto, poiché, anche sotto altri aspetti relativi alla protezione dei dati personali, la vicenda presenta vari profili di criticità, specie con riferimento all'osservanza dell'autorizzazione generale n. 8 sul trattamento dei dati genetici, nelle more del completamento degli approfondimenti curati dall'Ufficio, l'Autorità ha ritenuto necessario predisporre cautele idonee ad assicurare il rispetto dei diritti degli interessati (provv. 6 ottobre 2016, n. 389, doc. web n. 5508051). È stato, quindi, adottato un provvedimento di blocco nei confronti della società londinese, al fine di fronteggiare il rischio del verificarsi di un pregiudizio rilevante per gli interessati, consentendo così ai donatori di manifestare il proprio consenso al trattamento dei dati da parte della nuova società, ovvero esercitare i loro diritti con riferimento all'utilizzo dei dati e dei campioni contenuti nella biobanca (artt. 7, 13, 23, 90, 107, 110 del Codice e autorizzazione generale n. 8, punti 5 e 6).

Il blocco non riguarda, infatti, le operazioni di trattamento necessarie alla nuova società per garantire un'adeguata conservazione dei dati e dei campioni contenuti nella banca dati (ove, venute meno le esigenze cautelari, venga acquisita la disponibilità di questi ultimi), nonché per ricontattare i donatori, al fine di rendere loro l'informativa e raccogliere una nuova manifestazione di consenso,

oppure per fornire adeguato riscontro alle eventuali richieste degli interessati volte a esercitare i loro diritti in materia di protezione dei dati personali.

A fine 2016, inoltre, il Garante ha rinnovato l'autorizzazione generale sui dati genetici, in termini sostanzialmente analoghi alla precedente (provv. 15 dicembre 2016, n. 530, doc. web n. 5803688). Al pari delle altre, tale autorizzazione sarà efficace dal 1° gennaio 2017 fino al 24 maggio 2018, tenuto conto che a decorrere dal 25 maggio 2018 sarà applicabile il regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

7 La ricerca scientifica e la statistica

7.1. *La ricerca scientifica*

Registro tumori della Sardegna

Nel 2016 l'Autorità si è occupata dei registri di patologia, per gli aspetti relativi ai trattamenti di dati personali, anche sensibili, effettuati per la loro realizzazione e tenuta.

In tale ambito, il Garante ha espresso parere favorevole sullo schema di regolamento del registro tumori della Sardegna (provv. 25 febbraio 2016, n. 76, doc. web n. 4853986). Il testo, predisposto dalla Regione Sardegna, è stato uno dei primi in Italia a regolamentare, in linea con la normativa nazionale, i registri di patologia definendo le modalità di raccolta e trattamento dei dati anagrafici e sanitari delle persone affette da tumore e dei loro familiari, per finalità di studio e ricerca, nonché per una corretta stima epidemiologica ed economica della malattia.

Lo schema di regolamento, che tiene conto di molte delle osservazioni del Garante, determina, tra l'altro, quali dati contenuti nei registri delle tre macro aree, individuate in Sardegna, dovranno convergere nel registro unico regionale e stabilisce l'obbligo di informare i pazienti riguardo all'uso che verrà fatto dei loro dati sensibili. Il regolamento prevede, inoltre, l'adozione di particolari cautele a protezione dei dati riferiti ai malati di tumore (come, ad es., la pseudonimizzazione al fine di non rendere le informazioni personali immediatamente riconducibili al singolo malato), così come l'implementazione di misure organizzative e accorgimenti tecnici idonei a garantire la sicurezza delle informazioni.

Nel dare il suo parere, l'Autorità ha comunque chiesto ulteriori perfezionamenti del testo. Tra questi, la previsione che la titolarità del trattamento dei dati del registro dei tumori non sia riferibile alla Regione Sardegna, ma all'Osservatorio epidemiologico regionale, ovvero all'organo incaricato per legge del perseguimento degli scopi scientifici e di valutazione dell'assistenza sanitaria. In questo modo, solo gli operatori dell'Osservatorio potranno trattare dati personali sulle neoplasie dei singoli pazienti, mentre gli altri organi o uffici della Regione potranno consultare solo informazioni aggregate e anonime. Tra le misure indicate dall'Autorità, anche al fine di rafforzare la sicurezza informatica del registro, si menzionano l'utilizzo di meccanismi di autenticazione forte per consentire l'accesso ai dati al personale incaricato, nonché la conservazione separata dei dati anagrafici da quelli sanitari.

La necessità di garantire la riservatezza e l'integrità dei dati sensibili raccolti in queste banche dati è stata ribadita di recente dal presidente Soro, nel corso dell'audizione sulle proposte di legge recanti Istituzione e disciplina del Registro nazionale e dei registri regionali dei tumori, presso la Commissione affari sociali della Camera dei deputati. In questa occasione, il Presidente ha rimarcato l'importanza "di tracciare l'equilibrio migliore tra esigenze di analisi epidemiologica (che in ultima analisi significa diritto alla salute) e diritto alla protezione dei dati personali dei pazienti" ed evidenziato che "la perdita, la sottrazione, l'alterazione, l'abuso di un dato sanitario rende vulnerabili banche dati essenziali e, insieme, viola quanto di più intimo e privato vi è nella persona: ne tocca la dignità". "La carente sicurezza dei dati – ha aggiunto il Presidente – può rappresentare, in altri termini, una causa di malasanità; e la protezione dei dati personali, per converso, rappresenta un fattore determinante di efficienza sanitaria" (audizione 8 marzo 2016, doc. web n. 4762078; cfr. par. 3.1).

Registro veneto dialisi e trapianti

Sempre in materia di registri di patologia, è stato esaminato uno schema regolamento predisposto della Regione Veneto per disciplinare il funzionamento del registro dialisi e trapianti, istituito presso un'azienda sanitaria territoriale ed articolato in due sezioni: una dedicata ai casi di malattia renale cronica in dialisi e/o trapianto e di nefropatia diagnosticata con biopsia renale e un'altra relativa ai casi di sindrome nefrosica pediatrica. In attuazione della legge regionale, che prevede l'istituzione di taluni registri di patologia e di mortalità e, in conformità alle disposizioni del Codice sul trattamento dei dati sensibili da parte di soggetti pubblici, lo schema, sottoposto al parere dell'Autorità, individua i tipi di dati sensibili, le operazioni eseguibili, le specifiche finalità perseguite, i soggetti che possono avere accesso al registro, i dati che possono conoscere e le misure di sicurezza.

Il parere favorevole dell'Autorità è stato reso su una versione aggiornata dello schema di regolamento che tiene conto delle osservazioni formulate dall'Ufficio, integralmente recepite dalla Regione (provv. 15 settembre 2016, n. 354, doc. web n. 5497118). Le indicazioni hanno riguardato, tra l'altro, l'utilizzo dei soli dati aggregati per le finalità del registro di prevenzione, di programmazione sanitaria e di verifica della qualità delle cure; la raccolta del consenso per la trasmissione delle informazioni del registro a enti, istituti di ricerca e società scientifiche, ivi comprese quelle che curano la tenuta del registro italiano e del registro europeo di dialisi e trapianto; l'individuazione dei ruoli dei soggetti coinvolti nel trattamento dei dati; i modelli di informativa da rendere agli interessati contenuti negli allegati al regolamento. Inoltre, è stato chiesto di specificare le misure volte a garantire la protezione e l'esattezza dei dati, nonché le modalità e le operazioni che devono precedere l'elaborazione statistica e l'analisi epidemiologica delle informazioni contenute nel registro, tra le quali, la de-identificazione dei dati raccolti. Altre indicazioni hanno attenuto alla necessità di prevedere la verifica periodica circa l'adeguatezza delle misure di sicurezza, anche in caso di incidenti informatici (*data breach*). Tra le misure e gli accorgimenti disposti per tutelare la riservatezza dei pazienti, lo schema prevede, infine, l'utilizzo di codici identificativi e di tecniche di cifratura, nonché la conservazione separata dei dati anagrafici da quelli sanitari.

Il Garante ha ricordato inoltre che la regolamentazione statale in materia di registri di patologia e di sistemi di sorveglianza prevede, tra l'altro, che le regioni e le province autonome possano istituire, con propria legge, registri di patologia di rilevanza regionale e provinciale diversi da quelli individuati da un decreto del Presidente del Consiglio dei ministri, su proposta del Ministero della salute, previa intesa della Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome, acquisito il parere del Garante (v. art. 12, commi 10 ss., d.l. 18 ottobre 2012, n. 179 convertito con modificazioni dalla l. 17 dicembre 2012, n. 221). Al momento, tuttavia, tale decreto, sul cui schema si era espressa l'Autorità (provv. 23 luglio 2015, n. 435, doc. web n. 4252386), non risulta adottato, né è stato sottoposto all'esame del Garante, per il parere di competenza, il regolamento di attuazione al quale la legge demanda la definizione degli aspetti fondamentali del trattamento riguardanti le garanzie per la protezione dei dati trattati nei registri, in conformità alle disposizioni del codice sul trattamento di dati sensibili da parte di soggetti pubblici (v. art. 12, comma 13, d.l. n. 179/2012 cit. e art. 13, comma 2-*bis*, d.l. 21 giugno 2013, n. 69, convertito con modificazioni dalla l. 9 agosto 2013, n. 98).

Un altro caso ha riguardato la legge della Regione Calabria n. 2/2016 sull'istituzione del registro tumori della popolazione regionale, sulla quale l'Autorità ha fornito alla Presidenza del Consiglio dei ministri elementi di valutazione per l'eventuale impugnazione dinanzi alla Corte costituzionale ai sensi dell'art. 127 della Costituzione (cfr. par. 3.4).

Trattamento di dati sanitari di pazienti incapaci

In materia di trattamento a fini di ricerca di dati sulla salute riferiti a pazienti incapaci di prestare il consenso, il Garante ha rilasciato all'ospedale Guglielmo da Saliceto di Piacenza e ad altri centri di cura l'autorizzazione prevista dall'art. 110 del Codice. L'ospedale ha, in particolare, chiesto all'Autorità di poter trattare i dati dei pazienti, anche senza il loro consenso, qualora questi risultino temporaneamente incapaci di prestarlo, per effettuare uno studio osservazionale multicentrico sulle complicanze emorragiche in pazienti, in terapia con nuovi farmaci anticoagulanti, ricoverati in pronto soccorso (provv. 14 gennaio 2016, n. 5, doc. web n. 4727402).

Nel rilasciare l'autorizzazione, il Garante ha considerato il parere favorevole acquisito dal comitato etico, specie con riferimento alle modalità prospettate dal protocollo per il trattamento dei dati personali. Al riguardo, lo studio prevede che, nel caso in cui il medico della sperimentazione verifichi che il paziente si trovi in stato d'incoscienza e non sia in grado di comprendere l'informativa e di prestare un valido consenso al trattamento dei dati, il centro di cura cerchi, in ogni caso, di ottenere il consenso dai prossimi congiunti o familiari o dai rappresentanti dell'interessato oppure da un medico non associato alla ricerca. Qualora, poi, nel corso dello studio, le condizioni di salute dei pazienti migliorino, sarà raccolto il loro consenso alla continuazione della ricerca, previa idonea informativa.

Inoltre, secondo il protocollo dello studio, il trattamento dei dati personali sulla salute dovrà riguardare soltanto le informazioni e le operazioni strettamente indispensabili alla ricerca (quali quelle relative al sesso, alla data di nascita, al peso, all'altezza e i dati sulla salute registrati nelle cartelle cliniche). I medici si limiteranno a raccogliere e ad analizzare i dati clinici dei pazienti potendo, eventualmente, ricontattarli fino a novanta giorni dopo le dimissioni, per raccogliere altre informazioni sulle loro condizioni cliniche e su altre possibili complicanze insorte nel frattempo. I dati sanitari dello studio non saranno comunicati o trasferiti all'estero se non in forma rigorosamente aggregata e anonima e saranno resi pubblici solo in tale forma.

Il Garante ha precisato infine che la ricerca dovrà avvenire nel rispetto delle modalità previste nella richiesta di autorizzazione, anche per ciò che concerne la designazione dei soggetti che collaborano all'esecuzione dello studio, con l'adozione di idonee misure di sicurezza e la definizione del periodo di conservazione dei dati.

Progetti di ricerca europei

Sempre nel 2016, sono pervenute diverse richieste di approvazione, autorizzazione o nulla osta in merito a trattamenti di dati effettuati per l'esecuzione di progetti di ricerca finanziati dalla Commissione europea nell'ambito del programma Horizon 2020. Al riguardo, è stato precisato che il Garante è un'autorità di controllo della liceità e correttezza dei trattamenti di dati personali e che non rientra tra i suoi compiti la valutazione preliminare di progetti di ricerca o l'approvazione dei moduli utilizzati per la raccolta dei dati personali nell'ambito di singoli studi (nota 20 settembre 2016).

La disciplina di protezione dei dati personali prevede, infatti, il rilascio di un'autorizzazione preventiva dell'Autorità soltanto in alcuni casi tassativamente individuati dal Codice e, in particolare, per i trattamenti dei dati personali, diversi da quelli sensibili e giudiziari, che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato (art. 17). Inoltre, talune tipologie di trattamenti sono soggetti all'obbligo di previa notificazione al Garante, in quanto suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato (artt. 37 e 38 del Codice). Si tratta, in particolare, di trattamenti particolarmente delicati, come quelli di dati genetici o biometrici oppure di informazioni relative all'ubicazione di persone o oggetti, o anche di dati sulla salute utilizzati per particolari finalità sanitarie (procreazione assistita, prestazioni di servizi sanitari per via telematica relativi a banche di dati, indagini epidemiologiche, etc.), ovvero finalizzati a definire il pro-

filo o la personalità dell'interessato (v. al riguardo i chiarimenti forniti dal Garante il 23 e 24 aprile 2004, doc. web nn. 993385 e 996680).

Spetta pertanto al titolare del trattamento verificare se i trattamenti di dati personali previsti per la conduzione della ricerca rientrino tra le ipotesi che richiedono un'autorizzazione del Garante o una notificazione preventiva all'Autorità. Compete infatti a tale soggetto garantire che l'utilizzo dei dati personali a scopo di ricerca sia rispettoso delle regole in materia di protezione dei dati e dei princìpi fondamentali del trattamento.

Recapiti telefonici raccolti in precedenti progetti di ricerca

All'Ufficio è stato poi richiesto di fornire le proprie indicazioni in merito alla possibilità di utilizzare i recapiti telefonici forniti da pazienti coinvolti in progetti di ricerca ormai conclusi al fine di verificare la loro disponibilità ad aderire a nuovi studi. Al riguardo, è stato chiarito che non si ravvisano ostacoli a praticare tali modalità per contattare le persone interessate, purché sia resa un'idonea informativa e raccolto il consenso al trattamento dei dati che si intende effettuare a scopo di ricerca. Ciò, fermo restando che la possibilità utilizzare i dati sulla salute raccolti in precedenti progetti di ricerca e riferiti alle pazienti decedute o irreperibili, all'esito di ogni ragionevole sforzo compiuto per contattarle, è subordinato all'esistenza di presupposti previsti dall'autorizzazione generale n. 9 al trattamento dei dati personali per scopi di ricerca scientifica, tra i quali il parere favorevole del comitato etico territorialmente competente (provv. 15 dicembre 2016, n. 531, doc. web n. 5805552).

Con specifico riferimento alle prospettate modalità telefoniche per rendere l'informativa alle pazienti, è stato inoltre evidenziato che è necessario adottare soluzioni idonee a raggiungere la ragionevole certezza che la persona contattata sia effettivamente l'interessata e a scongiurare il rischio di un'indebita conoscenza dei suoi dati sanitari da parte di terzi rispondenti, impartendo agli incaricati opportune istruzioni affinché, nel qualificarsi, non facciano riferimento all'oggetto dello studio e chiedano innanzitutto di conferire direttamente con l'interessata (nota 2 dicembre 2016).

7.2. La statistica

Nel 2016 il Garante ha avviato l'esame dei trattamenti di dati personali effettuati nell'ambito del Programma statistico nazione (Psn) 2017-2019, fornendo all'Istat, nell'ambito di appositi incontri, prime indicazioni in ordine al rispetto del Codice e del codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (Sistan), All. A3 al Codice. Ciò ferma restando l'esigenza di sottoporre a una verifica preliminare dell'Autorità i sistemi informativi statistici per individuare adeguate garanzie volte ad assicurare l'applicazione dei princìpi in materia di protezione dei dati personali attraverso idonee misure ed accorgimenti (art. 17 del Codice).

Il Garante, su invito dell'Istat, ha inoltre partecipato, in qualità di osservatore esterno, ai lavori di una commissione tecnica sull'uso dei *big data* per la statistica ufficiale, con l'obiettivo di approfondire, per i profili di competenza, le problematiche derivanti dall'utilizzo delle fonti e dai rischi di reidentificazione degli interessati.

Con parere del 6 ottobre 2016 (n. 391, doc. web n. 5834597), l'Autorità si è anche pronunciata favorevolmente sul Programma statistico regionale 2014-2016-Aggiornamento 2015-2016 predisposto dalla Regione Emilia Romagna ai sensi del regolamento regionale 30 maggio 2014, n. 1 sul trattamento dei dati sensibili e giudiziari di competenza della Giunta della Regione Emilia-Romagna, delle aziende sanitarie, degli enti e delle agenzie regionali e degli enti vigilati dalla Regione e, in

7

particolare, sulla scheda 32 del predetto regolamento, relativa ai trattamenti non ricompresi nel Programma statistico nazionale effettuati per scopi statistici da soggetti Sistan (ufficio statistico della Regione).

Nel parere, il Garante ha ritenuto idonee le modalità semplificate per rendere l'informativa agli interessati attraverso il proprio sito internet istituzionale, prospettate dalla Regione nella richiesta di parere, ai sensi dell'art. 6, comma 2 del codice di deontologia.

8 I trattamenti da parte di Forze di polizia

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

A seguito di segnalazioni ricevute, l'Autorità ha assicurato anche quest'anno il riscontro da parte del Dipartimento della pubblica sicurezza del Ministero dell'interno e di uffici periferici della Polizia di Stato alle richieste degli interessati sia di accesso e comunicazione dei dati conservati presso il Centro elaborazione dati (Ced), sia di eventuale rettifica dei dati medesimi, nel rispetto delle disposizioni poste dall'art. 10, l. 1° aprile 1981, n. 121, come modificato dall'art. 175 del Codice.

8.2. *Altri interventi riguardanti le Forze di polizia*

Di particolare rilievo, nel 2016, l'attività relativa all'attuazione degli artt. 53 e 57 del Codice, in corso di svolgimento al momento in cui viene redatta questa Relazione.

Come noto, il comma 3 del menzionato art. 53 prevede che, con decreto adottato dal Ministro dell'interno, previa comunicazione alle competenti Commissioni parlamentari, sono individuati, nell'All. C al Codice, i trattamenti non occasionali di cui al comma 2 del medesimo articolo, effettuati con strumenti elettronici e i relativi titolari. Si tratta, in estrema sintesi, dei trattamenti che sono sottoposti ad un più snello regime di protezione dei dati personali, essendo svolti per finalità di polizia. Il Ministero dell'interno ha richiesto al Garante il parere in ordine ad uno schema di decreto di cui all'art. 53, comma 3, che in sostanza indica quali sono i trattamenti per finalità di polizia sottoposti al regime in parola.

Lo stesso Ministero ha inoltre richiesto il parere del Garante sull'attuazione dell'art. 57 del Codice, ossia sullo schema del regolamento, adottato con d.P.R., previa deliberazione del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro della giustizia, con il quale sono individuate le modalità di attuazione dei princìpi del Codice relativamente al trattamento dei dati effettuato per le finalità di cui all'art. 53. Il Ministero ha adottato due testi sull'attuazione dell'art. 57, il primo di carattere generale ed il secondo relativo alla disciplina dei trattamenti posti in essere dal Ced interforze del Ministero dell'interno. Su tali schemi di provvedimento si è svolta, in clima di piena collaborazione istituzionale, un'intensa attività di confronto con il proponente Ministero, nell'idea di definire nei primi mesi del 2017 i pareri di competenza del Garante.

Videosorveglianza dello stadio Olimpico di Roma

Per quanto riguarda la casistica, si segnala che con provvedimento 28 luglio 2016, n. 338 (doc. web n. 5386852) è stata definita la verifica preliminare sul sistema di videosorveglianza presso lo stadio Olimpico di Roma, richiesta dalla Questura di Roma ai sensi dell'art. 17 del Codice. Il sistema è provvisto di una funzione di riconoscimento facciale, che fornisce le immagini degli spettatori abbinate automaticamente al nominativo della persona risultante dal sistema di controllo degli accessi ai tornelli e dal sistema di biglietteria (i dati anagrafici dell'acquirente sono richiesti al momento dell'emissione dei biglietti per assistere alle partite di calcio). Il *software* confronta le immagini acquisite al momento del transito nei tornelli di accesso con

quelle riprese all'interno dello stadio durante gli eventi sportivi, in modo da risalire alla reale identità dell'autore di eventuali condotte delittuose. La Questura aveva rappresentato che l'esistente sistema di videosorveglianza, sebbene consenta agevolmente una visione complessiva dei flussi di persone e degli spalti interni, risulta insufficiente per una identificazione dei singoli responsabili di comportamenti vietati, rendendo perciò necessarie efficaci modalità tecniche per giungere alla compiuta identificazione dei responsabili di disordini senza esporre a rischio l'incolumità degli operatori di polizia e prospettando la conservazione delle immagini per sette giorni, ove non rilevanti ai fini di eventuali accertamenti su condotte illecite.

Il Garante ha ritenuto che il sistema proposto dalla Questura, pur comportando, in concreto, un'ingerenza nella sfera di autodeterminazione degli interessati e, conseguentemente, sui loro comportamenti, non arrechi comunque un pregiudizio rilevante per gli individui, ritenendo congruo il periodo di conservazione di una settimana indicata nel progetto. Ha però ravvisato l'esigenza di evitare rischi per i diritti e le libertà fondamentali degli interessati, vista la natura delle informazioni raccolte e le modalità di trattamento, ed a tal fine ha prescritto le idonee misure, ai sensi dell'art. 17 del Codice, che si applica anche ai trattamenti effettuati dalle Forze di polizia. In particolare è stato prescritto: che il sistema sia utilizzato direttamente ed esclusivamente da operatori appartenenti alle Forze di polizia, all'esclusivo fine di prevenzione, accertamento e repressione delle condotte per le quali è previsto il divieto di accesso ai luoghi dove si svolgono manifestazioni sportive, ovvero di più gravi reati; che le società delle quali si avvale il gestore dell'impianto siano designate responsabili del trattamento (art. 29 del Codice), fermo restando che le persone fisiche che trattano materialmente i dati, in particolare coloro che accedono al sistema per operazioni di manutenzione, devono essere designate incaricate del trattamento e devono essere loro impartite le necessarie istruzioni (art. 30 del Codice); che la protezione logica delle immagini sia assicurata da meccanismi di *strong authentication*. Qualora il Ministero dell'interno intenda collocare, per le finalità di cui sopra, impianti analoghi in altri stadi calcistici, non sarà necessario ricorrere ad una nuova verifica preliminare.

Case circondariali

Anche nel 2016 l'Autorità è stata più volte interpellata con riguardo ai trattamenti effettuati presso le case circondariali.

Sui sistemi di videosorveglianza installati presso case circondariali ha ribadito le indicazioni già dettagliatamente fornite nell'anno precedente, per le quali si fa rinvio alla Relazione 2015 (v. p. 89 e seg.).

L'Autorità ha poi fornito riscontro alla richiesta di una casa circondariale sulla possibilità di affidare, per conto di una Asl, ad una cooperativa di detenuti, il compito di procedere alla dematerializzazione di cartelle sanitarie. Al riguardo si è evidenziata l'esigenza di rispettare il Codice, in particolare designando quali responsabili del trattamento, ai sensi e per gli effetti dell'art. 29, i professionisti esterni incaricati del coordinamento delle operazioni di dematerializzazione, e quali incaricati del trattamento, nei modi e termini stabiliti dall'art. 30, le persone incaricate delle operazioni materiali di trattamento.

Infine si è intervenuti su un reclamo in merito alla comunicazione sistematica, da parte di una casa circondariale agli uffici della motorizzazione civile, delle patologie dei dipendenti ritenute influenti sulla capacità di conduzione di veicoli. L'Autorità, assunte le necessarie informazioni presso l'Amministrazione interessata, ha riscontrato che le comunicazioni erano riconducili al combinato disposto degli artt. 128, comma 1-quinquies e 119, comma 2, del codice della strada, relativi alla comunicazione agli uffici provinciali del Dipartimento per i trasporti del Ministero delle infrastrutture e dei trasporti di patologie incompatibili con l'idoneità alla guida. Il reclamo è stato pertanto archiviato.

8.3. *Il controllo sul sistema di informazione Schengen*

Il Ministero dell'interno-Dipartimento della pubblica sicurezza ha comunicato, con riferimento all'anno 2016, di aver posto in essere le misure che ancora al 2015 non risultavano attuate, tra quelle prescritte dal Garante per rafforzare la sicurezza nel trattamento dei dati effettuati per l'attuazione della Convenzione di Schengen (provv. 12 novembre 2009, doc. web 2330104).

Per quanto attiene agli adempimenti relativi ai provvedimenti prescrittivi, a suo tempo emanati dall'Autorità riguardo al cd. *disaster recovery*, si è preso atto di quanto sin qui realizzato in prima battuta nel complesso di Anagnina (Roma), a breve distanza dal centro principale di elaborazione dati, nonché dello stato di avanzamento del lavori nel sito presso il Centro polifunzionale della Polizia di Stato di Bari, individuato quale sede definitiva. Per quanto attiene alla figura del cd. *security manager*, è stato istituito presso il Dipartimento della pubblica sicurezza l'ufficio per la sicurezza dei dati ed è stato nominato il dirigente preposto.

Nel corso dell'anno sono stati forniti al riguardo ulteriori elementi, al vaglio dell'Autorità, circa l'idoneità delle misure poste in essere a soddisfare le prescrizioni impartite.

Com'è noto il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nel Sistema di informazione Schengen (SIS II), in virtù dei quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale dell'archivio Schengen, ossia al Dipartimento della pubblica sicurezza (cd. accesso diretto). Al riguardo, condividendo la raccomandazione formulata 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 solo dati idonei a monitorare le richieste degli interessati e l'attività di riscontro compiuta dalla Divisione NSIS.

Il numero 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.

Della terza valutazione Schengen dell'Italia in materia di protezione dei dati (le precedenti sono state nel 2004 e nel 2010), svoltasi nella settimana dal 14 al 18 marzo 2016, si riferisce in altra parte di questa Relazione (cfr. par. 24.3).

9 L'attività giornalistica

Permane costante l'attenzione dell'Autorità riguardo al rispetto dei diritti fondamentali degli interessati connesso allo svolgimento dell'attività di informazione e, più in generale, con riguardo alle varie forme di manifestazione del pensiero, in particolare in internet.

Al di là delle numerose interlocuzioni dell'Ufficio con le varie testate giornalistiche di volta in volta oggetto di segnalazione, cui di regola hanno fatto seguito interventi spontanei volti a rimuovere il contenuto di articoli o di informazioni eccedenti rispetto alla finalità informativa, non sono mancate le occasione nelle quali il Garante ha dovuto adottare decisioni puntuali su casi specifici (cfr. *infra* e par. 21.3).

Consiglio nazionale dell'Ordine dei giornalisti

In termini più generali, nel riscontrare favorevolmente l'iniziativa intrapresa dal Consiglio nazionale dell'Ordine dei giornalisti volta a riunire in un unico compendio le regole deontologiche che fanno capo al giornalista, con lo spirito di renderne più agevole la consultazione da parte di quanti attivamente operano nel mondo dell'informazione ed assicurarne così una maggiore effettività, il Presidente dell'Autorità ha sottolineato la necessità che le regole (anche di natura deontologica) non vadano disgiunte dalla loro aderenza alla realtà, specie se concernenti settori delicati quali quello dello svolgimento dell'attività giornalistica che massimamente incide su valori costituzionali propri dell'ordinamento nazionale ed europeo (nota Presidente 21 aprile 2016).

Nella stessa comunicazione è stata altresì rinnovata la necessità di un'opportuna opera di aggiornamento del codice di deontologia (risalente al 29 luglio 1998), data la rilevanza della dimensione digitale ed il crescente impatto di internet e dei *social network* sui diritti della persona, nonché alla luce degli effetti della sentenza della CGUE nel caso Google Spain (cd. *delisting*) e del diritto all'oblio previsto dal nuovo regolamento generale sulla protezione dei dati.

9.1. *I minori*

Non eccedenza

In linea con l'atteggiamento vigile, l'attenzione e lo scrupolo con i quali l'Autorità ha tradizionalmente condotto le verifiche in merito alla sussistenza dei requisiti di legittimità nel trattamento dei dati personali che riguardano i minori – atteso che un'irrispettosa diffusione dei dati stessi può determinare in capo agli interessati pregiudizio per la riservatezza e la dignità (in taluni casi compromettendone l'armonico sviluppo della personalità) – ha formato oggetto di approfondimento la diffusione da parte di alcune testate giornalistiche di una pluralità dati identificativi di una minore (nome, foto, età, luogo di residenza, denominazione della scuola frequentata) nonché di alcune informazioni puntuali sulla patologia da cui era affetta. In particolare, il Garante è intervenuto sulla diffusione della notizia di una minore che, per decisione dei genitori, aveva cessato di frequentare la scuola elementare in ragione degli asseriti maggiori rischi cui andava incontro, posto che alcuni suoi compagni non si erano sottoposti alle vaccinazioni volte a prevenire le malattie dell'infanzia. Pur riconoscendo l'interesse pubblico sotteso alla vicenda narrata (il dibattito in atto sul rapporto rischi/benefici delle vaccinazioni e la preoc-

cupazione manifestata dalla comunità scientifica riguardo a campagne di informazione volte a contestare la validità di tali forme di prevenzione), il Garante ha richiamato l'attenzione delle testate – che nel corso del procedimento hanno spontaneamente rimosso i dati identificativi della minore – sulle particolari garanzie poste a tutela dei minori e dei dati idonei a rivelare lo stato di salute (artt. 137 e 139 del Codice e artt. 7 e 10 del codice di deontologia), anche a mente di quanto stabilito al riguardo dalla Carta di Treviso, richiamata dal citato art. 7 del codice di deontologia (in caso di bambini malati, occorre porre "particolare attenzione e sensibilità nella diffusione delle immagini e delle vicende" che li riguardano al fine di evitare forme di sensazionalismo lesive della loro personalità). Nel caso di specie il consenso dei genitori (pur sussistente) non è stato ritenuto di per sé sufficiente a legittimare simili forme di pubblicità, dovendo il giornalista valutare autonomamente il carattere potenzialmente pregiudizievole del trattamento rispetto al minore e conseguentemente adottare tutte le cautele di volta in volta più opportune per tutelarlo, senza che questo significhi abdicare al ruolo fondamentale di denuncia e informazione della collettività circa notizie di interesse pubblico (provv. 21 aprile 2016, n. 176, doc. web n. 5029484).

Minori e "tavoli" aperti

Peraltro l'attività istituzionale dell'Autorità sulle tematiche relative al rapporto tra minori e mondo dell'informazione (tradizionale e sul web), non si esaurisce nell'attività di controllo, di regola (ma non necessariamente) svolto su impulso delle segnalazioni ricevute, ma è estesa alla partecipazione dell'Ufficio ad alcune iniziative istituzionali (tuttora in corso) volte a garantire un'informazione attenta rispetto al tema dei diritti dei minori e all'utilizzo consapevole e sicuro della rete da parte di questi ultimi: in questa cornice il Garante ha fornito un proprio contributo all'Autorità per le garanzie nelle comunicazioni in vista dell'aggiornamento del "Libro Bianco *Media* e Minori" ed è stato coinvolto, in ragione della specifica *expertise* maturata, nell'ambito di gruppi di lavoro (che vedono rappresentate varie competenze negli ambiti istituzionali e nel mondo dell'associazionismo) istituiti presso l'Osservatorio per il contrasto alla pedofilia e alla pornografia minorile (in base alla l. 6 febbraio 2006, n. 38) e presso l'Autorità garante per l'infanzia e l'adolescenza, con l'obiettivo di approfondire i temi della tutela del minore rispetto alle varie dimensioni della comunicazione (nella carta stampata, nei *media*, nel mondo digitale e nei *social network*).

9.2. *La cronaca giudiziaria*

Procedimento penale

Con il provvedimento del 24 novembre 2016, n. 489 (doc. web n. 5905569) è stata ritenuta legittima l'informazione fornita al pubblico da alcuni articoli di un quotidiano a diffusione prevalentemente locale concernente gli sviluppi di un processo penale a carico di una coppia, accusata di atti persecutori ai danni di familiari e conoscenti. Confermando il proprio orientamento, il Garante ha ritenuto – in ragione della gravità dei fatti contestati (atti persecutori, molestie, diffamazione), soggetti al vaglio del giudice penale, che vadano coinvolti una pluralità di persone, per lo più appartenenti alla ristretta cerchia familiare – che detti articoli di cronaca, riferendosi ad una vicenda di interesse generale, nel pur circoscritto ambito territoriale (un comune di poco più di 2.000 abitanti) di riferimento, fossero rispettosi della disciplina di protezione dei dati. In tale cornice, la scelta effettuata dai giornali di pubblicare anche i dati identificativi dei reclamanti, acquisiti lecitamente nel corso di pubbliche udienze, non è stata infatti ritenuta contraria al principio di essenzialità dell'informazione, anche in ragione della visibilità a livello locale degli

autori della condotta e della professione svolta da uno di essi, medico odontoiatra, e considerato il contesto di riferimento volto ad assicurare, nel rispetto della dignità individuale (cfr. art. 114, comma 6-*bis*, c.p.p., art. 8, commi 2 e 3, codice di deontologia), trasparenza e controllo da parte dei cittadini sull'attività di giustizia (al riguardo v. il documento del Garante 6 maggio 2004, "*Privacy* e giornalismo. Alcuni chiarimenti in risposta a quesiti dell'Ordine dei giornalisti", doc. web n. 1007634; in giurisprudenza cfr. Cass. civ., sez. I, 19 marzo 2008, n. 7261; Cass. civ., sez. III, 9 gennaio 2014, n. 194). Sotto diverso profilo, nel caso di specie il Garante non ha ritenuto si potesse utilmente invocare il diritto all'oblio ai fini di ottenere la cancellazione degli articoli in contestazione ovvero la loro deindicizzazione, trattandosi di notizie relative a vicende processuali recenti (sino all'anno in corso), per le quali si è ritenuto sussistente un interesse pubblico attuale (in tale senso, tra i tanti, provv. 21 aprile 2016, n. 187, doc. web n. 5146073 e le Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia española de protección de datos (AEPD) and Mario Costeja González" C-131/12, adottate dal Gruppo Art. 29, il 26 novembre 2014, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf).

Caso Vatileaks

Del pari, con riguardo alla diffusione a fini giornalistici del contenuto di sms scambiati tra una reclamante e un sacerdote – imputati nell'ambito di un procedimento penale avanti alle competenti Autorità vaticane e già componenti della Pontificia commissione referente di studio e indirizzo sull'organizzazione delle strutture economiche-amministrative della Santa Sede – nell'ambito di una vicenda (non solo) processuale che ha riscontrato ampia eco nell'opinione pubblica, il Garante ha ritenuto che gli elementi informativi oggetto di diffusione rientrassero nell'ambito del legittimo esercizio del diritto di cronaca, con particolare riguardo all'essenzialità dell'informazione rispetto a fatti di interesse pubblico (art. 137, comma 3, del Codice). Ciò anche muovendo dall'art. 6 del codice deontologico, secondo il quale le notizie che rivestono «rilevante interesse pubblico o sociale» possono essere divulgate "quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti". Peraltro, nel caso esaminato, da un lato non si è ritenuto che dal testo degli sms oggetto di pubblicazione emergessero dati idonei a rivelare la vita sessuale della reclamante (art. 4, comma 1, lett. *d*), del Codice); d'altro canto, si è reputato che il tenore dei messaggi, caratterizzati da un linguaggio immediato (e a tratti disinvolto), contribuisse ad evidenziare, secondo la prospettazione degli articoli di stampa, la natura della relazione intercorrente tra la reclamante ed il sacerdote, entrambi personalità particolarmente qualificate tanto da essere designate dal Sommo Pontefice quali componenti della menzionata commissione Pontificia. In questa cornice complessiva, i fatti a cui gli sms in questione si riferiscono e le relazioni che traspaiono tra i protagonisti degli stessi, sono stati ritenuti legati alla vicenda processuale connotata nel suo complesso come di interesse pubblico, così che la pubblicazione del testo di quei messaggi non è stata ritenuta riducibile ad una biasimevole attività di *gossip* giornalistico ma necessaria per fornire una completa informazione su fatti di interesse pubblico (provv. 27 aprile 2016, n. 193, doc. web n. 5202366).

Essenzialità dell'informazione

Con provvedimento del 14 luglio 2016, n. 305 (doc. web n. 5411527) è stata ritenuta in contrasto con il principio di essenzialità dell'informazione di cui agli artt. 137 del Codice e 6 del codice di deontologia, la pubblicazione, in articoli di cronaca reperibili anche *online*, dei dati identificativi di una donna sentita quale testimone nell'ambito di un procedimento penale a carico di un comandante provinciale

dei Vigili del fuoco per una missione effettuata da quest'ultimo a L'Aquila nel periodo *post* terremoto, viaggio a cui la stessa segnalante aveva preso parte (l'illecito contestato al comandante riguardava la circostanza che questi, in occasione della missione, avvalendosi dell'autovettura di servizio e del relativo autista, avesse effettuato per scopi personali tappe alternative, con sosta notturna in albergo). Il Garante ha ritenuto che la richiesta di tutela invocata fosse giustificabile in ragione della natura dei dati trattati, afferenti alle relazioni personali della segnalante con l'imputato, le quali non avevano comunque assunto alcuna autonoma rilevanza sul piano di eventuali responsabilità penali a carico della medesima e che quest'ultima invece aveva interesse a mantenere riservate; è stato pertanto prescritto alle testate interessate di adottare le misure necessarie al fine di assicurare l'anonimato della segnalante. Sotto un diverso profilo, peraltro, gli articoli oggetto di segnalazione non risultavano aggiornati alla luce della successiva assoluzione dell'imputato in merito agli aspetti oggetto della testimonianza resa dalla segnalante e al riguardo il Garante ha rappresentato la possibilità per l'interessato di esercitare i diritti di cui all'art. 7, comma 3, lett. *a*), del Codice, in linea peraltro con quanto affermato dalla Corte di cassazione (cfr. Cass. civ. sez. II, 5 aprile 2012, n. 5525).

9.3. *La diffusione delle informazioni* online

Integrazione dell'informazione

Numerose le istanze che continuano a pervenire in relazione a trattamenti di dati effettuati in modo lecito per finalità giornalistiche e oggetto di successive richieste degli interessati volte ad ottenere l'aggiornamento/integrazione dei dati personali che li riguardano quando eventi e sviluppi successivi abbiano modificato le situazioni oggetto di cronaca giornalistica (seppure a suo tempo corretta) incidendo significativamente sul profilo degli interessati che da tali rappresentazioni può emergere. In questo ambito può segnalarsi una decisione del Garante nella quale, richiamate le conclusioni cui è pervenuta la Corte di cassazione (sent. 5 aprile 2012, n. 5525) – secondo la quale "a salvaguardia dell'attuale identità sociale del soggetto occorre garantire al medesimo la contestualizzazione e l'aggiornamento della notizia già di cronaca che lo riguarda, e cioè il collegamento della notizia ad altre informazioni successivamente pubblicate, concernenti l'evoluzione della vicenda, che possano completare o financo radicalmente mutare il quadro evincentesi dalla notizia originaria, *a fortiori* se trattasi di fatti oggetto di vicenda giudiziaria, che costituisce anzi emblematico e paradigmatico esempio al riguardo" – si è prescritto agli editori di predisporre idonee misure nell'ambito dell'archivio storico, idonee a segnalare (ad es., a margine dei singoli articoli o in nota agli stessi) l'esistenza del seguito o dello sviluppo della notizia (nel caso di specie, la sopravvenuta archiviazione del procedimento giudiziario nei confronti del segnalante) in modo da assicurare all'interessato il rispetto del diritto all'identità personale, risultante dalla compiuta rappresentazione dei fatti che lo hanno visto protagonista (anche se solo in parte oggetto di cronaca giornalistica), fornendo così ad ogni lettore un'informazione attendibile e completa (provv. 15 settembre 2016, n. 358, doc. web n. 5515910).

Deindicizzazione

Con riferimento, invece, al reclamo nel quale si lamentava il rinvenimento sul web, mediante le ricerche effettuate grazie ad un motore di ricerca, di alcuni articoli risalenti al 2004 concernenti un'operazione antidroga e il conseguente arresto della reclamante per spaccio di sostanze stupefacenti, il Garante – in considerazione dell'intervenuta estinzione della pena a seguito di indulto nel 2010 e tenendo altresì conto delle "Guidelines on the implementation of the Court of justice of the European Union judgment on "Google Spain and Inc v. Agencia española de pro-

tección de datos (Aepd) and Mario Costeja González" C-131/12, WP 225 (cfr. par. 9.2), adottate dal Gruppo Art. 29 il 26 novembre 2014 (in particolare, con riguardo all'aspetto della pertinenza dell'informazione alla luce del tempo trascorso) nonché dell'orientamento della Corte di Cassazione, secondo la quale «il diritto dell'interessato a pretendere che proprie, passate vicende personali siano pubblicamente dimenticate, trova limite nel diritto di cronaca solo quando sussista un interesse effettivo ed attuale alla loro diffusione, nel senso che quanto recentemente accaduto trovi diretto collegamento con quelle vicende stesse e ne rinnovi l'attualità, diversamente risolvendosi il pubblico ed improprio collegamento tra le due informazioni in un'illecita lesione del diritto alla riservatezza» (Cass. civ., sez. III, 26 giugno 2013, n. 16111; cfr. altresì Cass. civ., sez. III, 5 aprile 2012, n. 5525) – ha prescritto la rimozione dai risultati del motore di ricerca degli url ottenuti inserendo quale chiave di ricerca il nominativo della reclamante (provv. 18 febbraio 2016, n. 64, doc. web n. 4798357; nello stesso senso provv.ti 25 novembre 2015, n. 623, doc. web n. 4664815; 21 maggio 2015, n. 306, doc. web n. 4203381; 25 giugno 2015, n. 384, doc. web 4220661).

Identità personale

Con provvedimento del 22 dicembre 2016, n. 546 (doc. web n. 5958184) il Garante si è pronunciato sulla segnalazione di un dipendente della Camera dei deputati che ha lamentato un trattamento illecito di dati personali in relazione a un servizio, trasmesso nel corso di una trasmissione televisiva e diffuso anche nella versione *online*, corredato da un'immagine che lo ritraeva in corrispondenza di un accesso di Palazzo Montecitorio, recante in sovraimpressione le scritte: "358 mila euro" e "Super stipendi alla Camera. I dipendenti vincono il ricorso". In linea con un precedente pronunciamento (provv. 15 novembre 2012, n. 344, doc. web n. 2185342), il Garante ha rilevato che, pur trattando il servizio un tema di rilevante interesse pubblico (le retribuzioni del personale gravanti sul bilancio dello Stato), ai fini della completezza dell'informazione, l'immagine identificativa del segnalante non costituiva un dato essenziale (art. 137, comma 3, del Codice e 6 del codice di deontologia), riferendosi il servizio giornalistico, in termini generali, all'intera categoria dei dipendenti della Camera dei deputati. Sotto diverso profilo, la particolare tecnica comunicativa impiegata – consistente nel sovrapporre la scritta relativa alla cifra sopra indicata sull'immagine del segnalante, assunto così a simbolo dell'intera categoria dei dipendenti della Camera dei deputati – era idonea a fornire un messaggio distorto, lesivo della dignità del segnalante (considerato il contesto negativo a cui la sua immagine risultava associata) e del diritto all'identità personale del medesimo (avendo il segnalante dichiarato l'inesattezza della cifra menzionata rispetto alla retribuzione da lui effettivamente percepita), situazioni giuridiche soggettive tutelate dal diritto alla protezione dei dati personali ai sensi dell'art. 2, comma 1, del Codice. Pur prendendo atto dell'avvenuta rimozione dell'immagine del segnalante dalla rete e dell'impegno ad astenersi per il futuro da ulteriori diffusioni dell'immagine dello stesso, il Garante ha prescritto all'editore titolare del trattamento di rettificare, con le modalità ritenute più opportune, la scritta sovraimpressa sull'immagine del segnalante – ove ancora presente negli archivi della testata – al fine di precisare che il trattamento economico evidenziato non corrispondeva a quello percepito dalla persona ritratta.

10 *Marketing*, profilazione e trattamento dei dati personali

10.1. *Verifiche preliminari e richieste di autorizzazione*

Beni di lusso

Nel corso del 2016 sono continuate a pervenire numerose istanze di verifica preliminare da parte di 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 indicati dal Garante nel provvedimento del 24 febbraio 2005 (doc. web n. 1103045). 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, tra l'altro, che i beni acquistati riguardano un genere particolare, di cd. fascia alta, con acquisti effettuati saltuariamente, sicché un periodo inferiore di conservazione avrebbe potuto determinare, nella sostanza, l'impossibilità di profilare la clientela (provv.ti 18 maggio 2016, n. 227, doc. web n. 5260385; 1° dicembre 2016, n. 501, doc. web n. 5890648).

Intermediazione immobiliare, creditizia e assicurativa

Analoghe esigenze sono state riconosciute rispetto al trattamento dei dati personali per finalità di profilazione e *marketing* da parte di operatori economici operanti nel settore dell'intermediazione immobiliare nonché nel correlato mercato della mediazione creditizia e assicurativa nel quale il cliente usufruisce di un servizio strumentale alla conclusione di un contratto di mutuo, finanziamento e/o assicurazione, con possibilità di conservare i dati per un periodo massimo pari a dieci anni, decorrente dalla registrazione degli stessi (cfr., rispettivamente provv.ti 30 giugno 2016, n. 285, doc. web n. 5411203 e 15 dicembre 2016, n. 534, doc. web n. 5958146).

Programmi televisivi e pubblicità "mirata"

Il Garante ha accolto una richiesta di verifica preliminare presentata da un operatore televisivo concernente la realizzazione di un progetto volto a veicolare messaggi pubblicitari diversi da quelli *standard* a gruppi distinti di spettatori, ciascuno dei quali aventi caratteristiche ben definite; in particolare, destinatari della pubblicità sono i nuclei familiari in possesso di uno specifico apparecchio per la ricezione da satellite o via internet, raggruppati in appositi *cluster* in base a caratteristiche relative al servizio fruito (ad es., tipologia del "pacchetto" tv, durata dell'abbonamento, modalità di pagamento) e ad altre informazioni (fascia di età, luogo di residenza). Al fine di assicurare il corretto trattamento dei dati personali, la società dovrà consentire a coloro che non intendono aderire al progetto, di potersi opporre in modo agevole (ad es., digitando "no" sul telecomando, spuntando una apposita casella nella sezione dedicata agli utenti registrati nel proprio sito web, oppure inviando una comunicazione, anche via *e-mail*, o interagendo con il proprio *call center*); gli utenti devono essere chiaramente informati delle finalità perseguite con il progetto oggetto di verifica preliminare e devono essere illustrate agli stessi le modalità impiegate per assicurare l'uso dei dati in forma aggregata, sì da non essere riconducibili ai singoli abbonati. Gli abbonati devono inoltre essere informati della possibilità di esercitare i diritti riconosciuti dalla normativa in materia di protezione dei dati (accesso ai dati, rettifica, cancellazione, opposizione al trattamento): tale informa-

tiva potrà essere resa in forma sintetica mediante un messaggio (ripetuto più volte, al fine di assicurarne la visibilità ai vari componenti della famiglia) che apparirà a video alla prima accensione dopo l'aggiornamento del *software* e che dovrà rimandare ad una pagina web, facilmente reperibile. Nell'informativa, oltre a fornire le informazioni sui diritti degli utenti, la società istante è tenuta a descrivere in dettaglio il progetto. L'utente che non intende ricevere gli *spot* "mirati" potrà opporsi in modo semplice, anche usando il telecomando (provv. 13 luglio 2016, n. 306, doc. web n. 5408313).

L'Autorità ha altresì valutato una richiesta di verifica preliminare presentata da una società specializzata in ICT (*Information and Communication Technology*) concernente la realizzazione di una piattaforma in grado di aggregare dati in forma anonima o anonimizzati provenienti da varie fonti, al fine di creare ed aggiornare dinamicamente una mappa comportamentale dei consumatori basata su modelli statistici di analisi e tale da consentire a soggetti che operano in mercati diversi (dai *media*, all'*e-commerce*, al web) di stimarne le metriche sui propri clienti ottimizzandone il profilo. I dati sarebbero stati acquisiti in parte da archivi pubblici liberamente accessibili, ma pure dalle società partecipanti al progetto, interessate a mettere a disposizione i profili (anonimi o anonimizzati) dei propri clienti per la costruzione di una mappa comportamentale più ampia e completa. L'Autorità ha in primo luogo ritenuto che, ove realmente i dati trattati fossero stati anonimi, alla fattispecie non avrebbe trovato applicazione la disciplina del Codice. Con riguardo, invece, ai trattamenti (preliminari) che avrebbero condotto alla anonimizzazione dei dati personali dei clienti-utenti da parte dei *data provider*, nonché ai trattamenti posti in essere dagli utilizzatori del servizio con riguardo alla fase (successiva rispetto alle operazioni poste in essere dalla società istante) della associazione alla propria clientela dei profili oggetto di elaborazione (o rielaborazione, in caso di riprofilazione) secondo le modalità descritte, è stata evidenziata la necessità di integrare gli elementi messi a disposizione del Garante da parte delle società partecipanti al progetto. Queste ultime, infatti, in qualità di titolari o contitolari del trattamento, sarebbero tenute a dare applicazione alla disciplina di protezione dei dati personali anzitutto in relazione, nel rispetto del principio di correttezza del trattamento (art. 11, comma 1, lett. *a*), del Codice), all'informativa da rendere agli interessati ai sensi dell'art. 13 del Codice, avendo cura di chiarire le finalità e le modalità del trattamento di anonimizzazione cui sarebbero stati destinati i dati personali dei clienti/utenti (in particolare quelle di profilazione e di riprofilazione) e le caratteristiche del processo, avuto riguardo anche al coinvolgimento dei diversi soggetti fruitori della piattaforma; all'acquisizione del consenso degli interessati alla profilazione, nel caso di specie per finalità di *marketing*; nonché all'obbligo di notificazione del trattamento di profilazione ai sensi dell'art. 37, comma 1, lett. *d*), del Codice (nota 7 aprile 2016).

Autorizzazione al trattamento di dati sensibili

Menzione a parte merita la richiesta di autorizzazione al trattamento di dati sensibili, formulata da una società operante nel settore della produzione e distribuzione di prodotti per l'igiene personale (nel caso di specie raccolti nell'ambito di un programma di fidelizzazione attraverso il proprio sito web e concernenti le condizioni individuali di salute, segnatamente l'incontinenza, della propria clientela) per finalità di profilazione e *marketing*, ai sensi degli artt. 26 e 41 del Codice, previa informativa *ex* art. 13 del Codice e con l'acquisizione del consenso scritto degli interessati, ai sensi dell'art. 26 del Codice. Ritenuto che la fattispecie in parola non rientrasse nell'ambito delle autorizzazioni generali già adottate, il Garante (tenendo in considerazione la raccomandazione adottata il 23 novembre 2010 dal Comitato dei ministri del Consiglio d'Europa CM/Rec (2010)13 sulla tutela delle persone fisiche con riguardo

al trattamento automatizzato di dati personali nel contesto della profilazione, con particolare riferimento al punto 3.1), dopo aver indicato con precisione la tipologia di dati suscettibili di trattamento per la predetta finalità di profilazione alla luce del principio di indispensabilità, ha individuato in un anno il tempo massimo di conservazione dei dati idonei a rivelare lo stato di salute trattati per la menzionata finalità (provv. 17 marzo 2016, n. 126, doc. web n. 4988333).

10.2. *L'attività di controllo dell'Autorità*

Migliaia sono state le segnalazioni pervenute in materia di *marketing* indesiderato (per un'analisi di dettaglio v. tab. 1, sez. IV), nella stragrande maggioranza riferite al *telemarketing*, quindi all'invio di comunicazioni commerciali via *e-mail* o sms: dal punto di vista (anche solo) quantitativo si tratta dell'area che va a comporre il "carico" assolutamente prevalente dell'Autorità, con una tendenza che, in particolare con riguardo a taluni operatori, non sembra dare segnali tangibili di flessione.

Dall'analisi delle segnalazioni pervenute nel settore del *telemarketing* è dato desumere che esse interessano sia gli abbonati iscritti nel registro pubblico delle opposizioni (Rpo) 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 sono occupati principalmente da due tipologie preminenti, quello delle società che offrono servizi di telefonia e quello delle *utilities* (in particolare gli operatori del settore energetico), con una differenziata consistenza numerica delle segnalazioni rispetto a ciascuno degli operatori.

Sono frequenti, inoltre, le telefonate promozionali effettuate, in violazione di legge, con numerazione chiamante oscurata come pure quelle rispetto alle quali si lamenta l'esecuzione da parte di operatori stabiliti al di fuori dell'Unione europea.

Sotto diverso profilo, viene costantemente segnalato il mancato o tardivo riscontro con riguardo all'esercizio dei diritti degli interessati da parte dei soggetti nel cui interesse si lamentano essere effettuate le comunicazioni promozionali (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); al di là del diritto di opposizione all'ulteriore trattamento dei dati per finalità di *marketing*, viene ripetutamente lamentato che non vengono fornite le necessarie indicazioni circa l'origine dei dati, indicazione imprescindibile al fine di consentire all'interessato di risalire agli archivi che stanno a monte delle comunicazioni telefoniche indesiderate.

Le incrementate verifiche

La persistenza (se non l'aumento) del fenomeno nel tempo (con polarizzazione su alcuni degli operatori oggetto di segnalazione), il percepito fastidio diffuso (al limite, in taluni casi, dell'esasperazione) di quanti effettuano le segnalazioni all'Autorità (e si tratta solo della punta dell'*iceberg*), 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 del Garante in questo contesto (peraltro con una penalizzazione di altri ambiti, pur di primaria rilevanza per l'assolvimento dei compiti istituzionali). Tale accentuato impegno ha comportato un incremento dell'attività di controllo da parte dell'Autorità, con verifiche ispettive *in loco* e presso i principali committenti, verifiche che solo in parte sono state definite nel 2016 con provvedimenti di divieto ed inibitori (v. *infra*), atteso che gli esiti di altri accertamenti, pure effettuati, continueranno nel 2017 e sono allo stato in fase di valutazione.

Il riscontro ai segnalanti

Sotto diverso profilo, ma si tratta di attività parimenti significativa, l'Ufficio ha provveduto a riformulare le FAQ presenti sul sito web dell'Autorità (doc. web n. 1794339) e ha dato riscontro individualizzato a larga parte delle migliaia di segnalazioni pervenute nel 2016 soprattutto al fine di fornire informazioni corrette sugli strumenti messi a disposizione dall'ordinamento a vantaggio degli interessati per prevenire od opporsi alle telefonate indesiderate (anzitutto esercitando i diritti di cui all'art. 7 del Codice anche avvalendosi del modello predisposto dall'Autorità, doc. web n. 1089924). In questa prospettiva, nelle comunicazioni individuali si è chiarito che i destinatari delle telefonate promozionali, quantomeno in taluni casi, potrebbero essere stati contattati lecitamente, sulla base di un consenso dagli stessi 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 il caso dei portali lavoro, v. provv. 5 maggio 2016, n. 206, doc. web n. 5185000); sulla base di tale consenso – talora illegittimamente acquisito, come nei casi di cd. consenso obbligato (cfr. par. 10.4) – le numerazioni telefoniche formano oggetto di comunicazione a (più) operatori economici e, quindi, alimentano, in un processo circolare, il flusso dei contatti promozionali.

Comunicazione istituzionale e audizioni del Garante

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 *telemarketing* selvaggio, presso la 8ª Commissione permanente – Lavori pubblici, comunicazioni – del Senato della Repubblica, 16 novembre 2016, doc. web n. 5661956).

10.3. *Telefonate e sms indesiderati a contenuto promozionale*

Telemarketing

È all'interno di questa complessiva cornice di riferimento che, a seguito di una dettagliata segnalazione pervenuta all'Autorità e considerato il numero elevato di quelle relative all'attività di *teleselling* nei confronti di uno dei principali operatori nazionali di telefonia – concernenti l'effettuazione delle chiamate in assenza di consenso degli interessati, la persistenza delle stesse nonostante l'iscrizione delle proprie utenze nel registro pubblico delle opposizioni e persino la loro effettuazione in tempi successivi all'esercizio del diritto di opposizione nei confronti di detto operatore telefonico – sono stati effettuati approfonditi accertamenti ispettivi (estesi ad alcuni *call center* in *outbound*) con la conseguente adozione di un provvedimento del Garante con il quale è stato accertato l'illecito trattamento di circa 2.000.000 numerazioni residenziali (per circa 400.000 contatti utili), avendo la società contattato sistematicamente nel 2015 «l'intera base dati di clienti "cessati e non consensati" […] al fine di verificare la possibilità di recuperare il consenso all'attività di *marketing*» (provv. 22 giugno 2016, n. 275, doc. web n. 5255159). Con riguardo a tale vicenda, l'Autorità ha verificato che dette numerazioni hanno formato oggetto di trattamento (e contatto mediante *call center*) nell'ambito di un'ampia campagna promozionale dedicata al "recupero consensi" per il trattamento dei dati per finalità promozionali dei clienti della società che non lo avevano in precedenza manifestato o, come nel caso segnalato, lo avevano espressamente negato, interessando le utenze per le quali la società «non disponeva del consenso individuale ad effettuare le

telefonate a contenuto promozionale» (provv. cit., punto 8.1). Nell'ambito del provvedimento in parola, il Garante ha altresì rilevato che la società, oltre a rendersi autrice delle violazioni di legge sopra richiamate rispetto ad una platea amplissima di interessati, ha al contempo posto in essere una condotta contraria alla prescrizione già impartita nei suoi confronti con il provvedimento 30 maggio 2007 (doc. web n. 1412598), in base alla quale era tenuta ad adottare "le misure necessarie per rendere il trattamento dei dati conforme alle disposizioni vigenti per ciò che concerne, specificamente, la possibilità di effettuare chiamate di carattere pubblicitario, promozionale o commerciale solo nei confronti di soggetti per i quali risulti documentato in modo adeguato il preventivo consenso informato rispetto al contatto telefonico […]". Di tale prescrizione la società non ha in concreto tenuto conto in relazione alle utenze oggetto della campagna "recupero consenso" che pure si è svolta in difformità rispetto alle regole di condotta stabilite internamente.

Nel provvedimento in esame, oltre al divieto di trattare ulteriormente i dati riferiti ai segnalanti nonché a quelli relativi alle utenze oggetto della campagna "recupero consenso" per finalità promozionali, ivi compresi i dati di coloro che, a seguito di tale trattamento illecito, avessero prestato il proprio consenso, il Garante ha espresso censure anche in relazione alle modalità di riscontro da parte della società alle richieste volte a far valere i diritti di cui all'art. 7 del Codice, ed in particolare il diritto di opposizione da parte dell'interessato al trattamento dei dati personali per finalità promozionali. In particolare, è stata ritenuta non conforme alla disciplina di protezione dei dati l'esclusione di taluni canali comunicativi da parte dell'interessato per l'esercizio dei diritti di cui all'art. 7, segnatamente la previsione per cui "l'opposizione non può essere effettuata tramite *e-mail* e/o pec", atteso che ciò si pone in contrasto con l'art. 8, comma 1, del Codice, secondo il quale i diritti di cui all'art. 7 del Codice possono essere esercitati "con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato […]" e con l'art. 9, comma 1, del Codice, secondo il quale "la richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica". Sotto diverso profilo, hanno formato oggetto di censura anche le modalità operative utilizzate per tenere conto delle istanze degli interessati dal punto di vista, anzitutto, della tempestività del riscontro: a questo riguardo, l'art. 8, comma 1, del Codice, prevede infatti che idoneo riscontro sia fornito all'interessato "senza ritardo". Infine è stato censurato il mancato inserimento in *black list* o in liste di non contattabilità dei dati personali dei "non clienti" (*prospect*), che venivano invece invitati ad iscriversi nel registro delle opposizioni: a questo riguardo si è osservato che tale prassi non trova alcun riscontro nella legge, atteso che il diritto di opposizione previsto dall'art. 7, comma 4, lett. *b*), del Codice, non può in alcun modo essere soggetto alla condizione della previa iscrizione dell'utenza nel registro pubblico delle opposizioni (iscrizione che, peraltro, ricorrendo talune condizioni, non potrebbe neanche essere pretesa dall'interessato).

Più in generale il Garante ha ricordato che, risiedendo il "nucleo duro" del diritto alla protezione dei dati personali nell'esercizio dei diritti previsti dall'art. 7 del Codice, le discipline di protezione dei dati personali si caratterizzano per il *favor* verso l'esercizio delle ricordate situazioni giuridiche soggettive tutelate (in tal senso depongono, oltre alle disposizioni sopra richiamate, la gratuità del diritto d'accesso, come pure l'art. 10 del Codice, secondo il quale "per garantire l'effettivo esercizio dei diritti di cui all'art. 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare: a) ad agevolare l'accesso ai dati personali da parte dell'interessato […]; b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente […]"), sì che le misure tecnico-organizzative che ciascun titolare del

trattamento, ivi compresa la società, è tenuto a porre in essere devono essere ispirate a questi princìpi. Al di là delle puntuali disposizioni richiamate, la cui violazione comporta l'illiceità del trattamento, si è altresì rilevato che le condotte che ostacolano o comunque determinano un più oneroso esercizio dei diritti per l'interessato rispetto al paradigma fissato dal legislatore integrano, in capo al titolare del trattamento, una violazione del principio di correttezza sancito all'art. 11, comma 1, lett. *a*), del Codice. Considerate le violazioni rilevate, salva l'adozione delle misure tecnico-organizzative idonee a garantire il tempestivo ed effettivo riscontro all'interessato che ha esercitato uno dei diritti di cui all'art. 7 del Codice, con particolare riferimento al diritto di opposizione al trattamento per finalità di *marketing* secondo quanto previsto dalla legge, il Garante ha prescritto, quale misura opportuna, che la società fornisca all'interessato il riscontro dovuto su un supporto durevole (ad es., mediante comunicazione scritta, sms, *e-mail*, etc.) ovvero, con riguardo all'esercizio dei diritti in forma orale (rispetto al quale l'incaricato già deve provvedere ad apposita annotazione ai sensi dell'art. 9, comma 1, del Codice), che gli venga comunicato un codice univoco di conferma (*ticket*).

Sms

Sulla base degli accertamenti che hanno condotto all'adozione del provvedimento testé menzionato è stato altresì possibile definire una distinta istruttoria nella quale nei confronti della medesima compagnia telefonica è stato accertato un trattamento illecito di dati per finalità di *marketing* mediante l'invio di sms, in tempi successivi rispetto all'esercizio del diritto di opposizione da parte del segnalante, che la società non aveva tempestivamente registrato nei propri sistemi (provv. 21 luglio 2016, n. 317, doc. web n. 5436585).

Verifiche analoghe sono state svolte nei confronti di altra primaria compagnia telefonica a seguito delle segnalazioni pervenute concernenti la ricezione da parte della stessa di sms indesiderati a contenuto promozionale con i quali pure si invitava la clientela che non aveva manifestato il consenso ai contatti commerciali e promozionali a farlo (provv. 27 ottobre 2016, n. 437, doc. web n. 5727908). È stato così possibile acclarare l'effettuazione, a far data dal 2015, di una pluralità di campagne, che hanno complessivamente coinvolto un numero pari a circa 5.000.000 di utenze mobili, volte all'acquisizione del consenso all'impiego delle utenze telefoniche per finalità di *marketing* ed effettuate in violazione di quanto previsto dall'art. 130, commi 1 e 2, del Codice. Esse hanno interessato due tipologie di clienti: quelli oggetto di nuova acquisizione e quelli già presenti nella *customer base* della società. All'esito delle verifiche è stato quindi vietato alla società di trattare ulteriormente per finalità promozionali i dati personali concernenti le utenze oggetto delle menzionate campagne, salvo che per quanti abbiano prestato il proprio consenso per le menzionate finalità promozionali decorso l'intervallo temporale indicato nei messaggi sms loro inviati.

Anche nel caso in esame, nel prescrivere che la società dia tempestivo riscontro all'esercizio dei diritti da parte degli interessati, il Garante ha altresì prescritto che l'interessato ottenga detto riscontro su un supporto durevole (ad es., mediante comunicazione scritta, sms, *e-mail*, etc.) ovvero, con riguardo all'esercizio dei diritti esercitato in forma orale, comunicando allo stesso un codice univoco di conferma (*ticket*).

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

Se sono sostanzialmente scomparse le istanze relative all'invio di fax indesiderati, numerosissime permangono le segnalazioni concernenti l'invio di comunicazione elettroniche automatizzate a contenuto promozionale, tematica da tempo all'atten-

zione del Garante (cfr. linee guida in materia di attività promozionale e contrasto allo *spam,* 4 luglio 2013, n. 330, doc. web n. 2542348, e già il provv. generale 29 maggio 2003 in materia di *spam*, doc. web n. 29840); rispetto ad esse, privilegiando le segnalazioni maggiormente dettagliate, sono stati attivati numerosi procedimenti, in materia di *e-mail marketing*, fenomeno di dimensioni rimarchevoli che si caratterizza per la (fastidiosa) persistenza dell'invio delle comunicazioni anche in tempi successivi rispetto all'esercizio del diritto di opposizione, spesso inutilmente reiterato da parte degli interessati e talvolta nonostante le rassicurazioni fornite dal titolare del trattamento; non di rado viene anche lamentato all'Autorità il mancato funzionamento dei *link* (talora) presenti nelle comunicazioni in parola, prassi di per sé scorretta e non conforme a quanto previsto dall'art. 11, comma 1, lett. *a*), del Codice (provv. 6 ottobre 2016, n. 390, doc. web n. 5834805).

Ancorché, per la quantità delle segnalazioni e la più incisiva interferenza nella tranquillità individuale, sul fenomeno del *telemarketing* (come si è detto) si sono focalizzati gli sforzi dell'Autorità, non pochi accertamenti *in loco*, anche con l'ausilio prezioso del personale del Nucleo speciale *privacy* della Guardia di finanza, sono stati effettuati e hanno consentito di adottare provvedimenti significativi in materia (anzitutto per il numero dei soggetti coinvolti dalle pratiche illecite di *spam*), con la conseguente attivazione di procedimenti sanzionatori (anche nei casi in cui non si è resa necessaria l'adozione di un provvedimento del Garante).

Entro questa cornice, con provvedimento 11 febbraio 2016, n. 49 (doc. web n. 4885578) adottato nei confronti di due distinte società che si sono rese autrici dell'invio di *e-mail* indesiderate a contenuto promozionale nei confronti del medesimo segnalante, il Garante, prescrivendo l'adozione delle misure necessarie a garantire il rispetto del diritto di opposizione al trattamento per finalità di *marketing* (art. 7, comma 4, lett. *b*), del Codice), ha vietato, al di là della vicenda individuale oggetto di segnalazione, l'ulteriore trattamento per finalità di *marketing* dei dati personali registrati nei *database* in assenza di un'idonea informativa ai sensi dell'art. 13 del Codice e del consenso informato degli interessati di cui all'art. 130, commi 1 e 2, del Codice (in un caso, vietandone altresì la comunicazione a terzi in violazione degli artt. 13 e 23 del Codice).

Consenso "obbligato"

Affrontando il caso di un utente che lamentava la ricezione, mediante l'utilizzo non autorizzato del proprio indirizzo *e-mail*, di una *newsletter* a carattere promozionale proveniente dall'indirizzo di posta elettronica di una società operante nell'*e-commerce* di articoli medicali (e pervenuta dopo l'acquisto *online* di alcuni prodotti sul sito della società), il Garante ha riaffermato l'illiceità del trattamento di dati per finalità di *marketing* in base al cd. consenso obbligato dell'interessato. Dalle verifiche effettuate, infatti, è emerso che gli utenti non solo non potevano esprimere tramite il sito web il necessario specifico consenso per le finalità di *marketing*, ma, più radicalmente, erano impossibilitati a procedere all'acquisto di un prodotto senza aver prima fornito un generico consenso al "trattamento dei dati personali". Nel caso di specie, peraltro, anche l'informativa fornita dalla società presentava profili di inidoneità, non specificando le modalità di contatto per lo svolgimento di attività a contenuto promozionale. Il Garante ha quindi vietato, al di là del caso oggetto di segnalazione individuale, l'ulteriore trattamento per finalità di *marketing* dei dati personali raccolti, prescrivendo la riformulazione del *form* di acquisizione del consenso degli interessati, l'integrazione del testo con le modalità utilizzate per il contatto promozionale e, infine, l'adozione delle misure opportune affinché la manifestazione del consenso da parte degli interessati al trattamento per finalità di *marketing* non sia condizione per il perfezionamento del contratto via web (provv. 10 marzo 2016, n. 110, doc. web n. 4988238).

10

Che la pratica (illegittima) del cd. consenso obbligato sia ricorrente è stato constatato dal Garante anche nella decisione assunta per tutelare da comunicazioni promozionali non richieste gli utenti dello sportello *online* di un fornitore di servizi energetici che, per usufruire dei servizi *online* (ad es., quelli connessi alla gestione della propria scheda anagrafica, all'andamento dei consumi e alla fatturazione direttamente sul sito web), venivano obbligati a rilasciare il consenso a ricevere comunicazioni promozionali (barrando un unico *check box* per un consenso onnicomprensivo al trattamento dei dati personali, sia per le finalità legate alla gestione del contratto – per le quali la legge non richiede tale adempimento – sia per la ricezione di messaggi di posta elettronica contenenti pubblicità o altro materiale promozionale). Peraltro, nel corso dell'istruttoria, è stato accertato che il ramo aziendale di fornitura del gas era stato acquisito da un'altra società che non aveva provveduto, come previsto dalla normativa, a inviare ai nuovi clienti l'informativa relativa al trattamento dei dati personali. Il Garante ha quindi vietato al primo operatore energetico, che aveva predisposto lo sportello per i servizi *online*, di utilizzare per finalità di *marketing* i dati personali di cui era ancora in possesso in assenza di un valido consenso; ha invece prescritto alla società cessionaria del ramo gas di provvedere senza ritardo a informare i clienti sulle modalità di trattamento dei dati loro riferiti (provv. 27 ottobre 2016, n. 439, doc. web n. 5687770).

E-mail grabbing

Non diversamente è stato ritenuto illecito il trattamento dei dati personali concernenti l'indirizzo di posta elettronica presente nel sito web del segnalante, e raccolto in assenza del consenso informato dello stesso (ed anzi, nel caso di specie, contro la chiara volontà negativa puntualmente espressa dal segnalante) in vista del successivo utilizzo per finalità promozionali dei dati personali per l'invio di comunicazioni indesiderate in violazione di quanto previsto dall'art. 130, commi 1 e 2, del Codice (in materia cfr., tra i tanti, i provv.ti 13 maggio 2015, doc. web n. 4337465; 25 settembre 2014, doc. web n. 3457687; 9 gennaio 2014, doc. web n. 2904350). Consenso preventivo (oltre che, informato, libero e specifico) che deve sussistere anche quando i dati personali (come, nella fattispecie, l'indirizzo di posta elettronica del segnalante) siano rinvenibili in internet, in quanto l'agevole reperibilità di tali dati non ne autorizza il trattamento per qualsiasi scopo, ma soltanto per le specifiche finalità sottese alla loro pubblicazione. Né, infine, il Garante ha ritenuto sufficiente avvisare i destinatari delle comunicazioni a contenuto promozionale della possibilità di opporsi a ulteriori invii (come nel caso in esame), atteso che tale accorgimento può trovare applicazione solo nell'ipotesi prevista dall'art. 130, comma 4, del Codice, fattispecie inconferente con la vicenda oggetto di segnalazione (non risultando alcun acquisto di prodotti o servizi della società da parte del segnalante, né l'invio di *e-mail* promozionali aventi ad oggetto prodotti o servizi analoghi a quelli in precedenza forniti). Per tali complessive ragioni il Garante ha vietato l'ulteriore trattamento per finalità di *marketing* dei dati personali trattati in assenza di un'informativa idonea e di un consenso legittimamente manifestato (ai sensi dell'art. 130, commi 1 e 2, del Codice), con riguardo sia al segnalante, sia ad altri soggetti i cui dati personali siano stati acquisiti con le modalità descritte nel provvedimento; ha inoltre prescritto l'adozione delle opportune misure tecniche ed organizzative affinché venga assicurata la piena attuazione dei diritti degli interessati di cui agli artt. 7 ss. del Codice, con particolare riferimento al diritto di opposizione al trattamento per finalità di *marketing* di cui all'art. 7, comma 4, lett. *b*), del Codice (provv. 6 ottobre 2016, n. 390, doc. web n. 5834805).

A conferma della prassi diffusa, ancorché illegittima, di utilizzo degli indirizzi di posta elettronica reperiti in internet per il loro successivo utilizzo quale indesiderato veicolo di comunicazioni a contenuto promozionale, merita anche di essere ricor-

dato il provvedimento 6 ottobre 2016, n. 390 (doc. web n. 5834805), nel quale si è ribadito che il requisito del consenso preventivo (oltre che, informato, libero e specifico) sussiste anche quando i dati personali (nella fattispecie, l'indirizzo di posta elettronica) siano rinvenibili in internet, in quanto l'agevole reperibilità di tali dati ne autorizza il trattamento unicamente per le specifiche finalità sottese alla loro pubblicazione (come costantemente ribadito dal Garante a partire dal provv. 11 gennaio 2001, doc. web n. 40823 e, quindi, con il provv. generale sullo *spamming* 29 maggio 2003, doc. web n. 29840; v. altresì le menzionate linee guida *spam*, par. 2.5).

Portale lavoro

Verifiche di analoga natura sono altresì state effettuate nei confronti di una società che gestisce un portale di intermediazione del lavoro – materia che aveva già formato oggetto in passato di intervento del Garante con provv. 5 dicembre 2013, n. 547, doc. web n. 2865637 (confermato da Trib. Como, sez. I civ., 22 ottobre 2014), con conseguente ordinanza di ingiunzione dell'11 giugno 2015, n. 349 (doc. web n. 4243173) – a seguito di una segnalazione relativa alla ricezione di una pluralità di messaggi di posta elettronica indesiderati a contenuto promozionale aventi ad oggetto beni e servizi di contenuto vario (non correlati con la ragione per la quale lo stesso aveva conferito i propri dati nel portale). Sotto diverso profilo, è stato altresì lamentato che, nonostante la presenza nell'ambito dei messaggi di un *link* per richiedere la cancellazione dall'indirizzario (*mailing list*), tale misura si rivelava in concreto inefficace atteso che, nonostante la richiesta di rimozione dall'indirizzario, continuavano a pervenire ulteriori comunicazioni di posta elettronica. Sulla base delle verifiche condotte – che hanno consentito di accertare che per fruire dei servizi finalizzati alla ricerca di lavoro (registrando i profili individuali ed il *curriculum vitae*), era obbligatorio accettare *in toto* le condizioni contenute nell'informativa sul trattamento dei dati, fornendo un unico consenso al loro trattamento per tutte le finalità in essa indicate (comprese quelle promozionali) pena l'impossibilità di portare a termine la procedura di registrazione – il Garante ha ritenuto violata, sotto più profili, la disciplina di protezione dei dati personali: da un lato, in relazione alla persistente trasmissione di messaggi a contenuto promozionale in date successive alla richiesta di cancellazione formulata dall'interessato; d'altro canto, più radicalmente, in ragione dell'impossibilità per gli interessati di manifestare liberamente e specificamente il consenso all'utilizzo dei dati personali per finalità promozionali (statuizione, quest'ultima, peraltro ripetutamente affermata dall'Autorità: provv.ti 20 dicembre 2012, doc. web n. 2223607; 15 luglio 2010, doc. web n. 1741998; 13 maggio 2015, n. 291, doc. web n. 4337465; 1° ottobre 2015, n. 508, doc. web n. 4452896).

Conseguentemente è stato vietato alla società l'ulteriore trattamento per finalità promozionali dei dati personali raccolti in occasione dell'iscrizione al "portale lavoro" in assenza della documentata acquisizione di un loro consenso libero e specifico e ha prescritto l'adozione delle opportune misure tecnologiche affinché la manifestazione del consenso da parte degli interessati al trattamento dei dati per finalità di *marketing* non sia condizione necessaria ai fini dell'esecuzione dei servizi resi tramite il sito web della società (provv. 5 maggio 2016, n. 206, doc. web n. 5185000).

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

Innovando la previgente disciplina in materia di localizzazione in Paesi terzi dell'attività di *call center*, la l. 11 dicembre 2016, n. 232 (Bilancio di previsione dello Stato per l'anno finanziario 2017 e bilancio pluriennale per il triennio 2017-2019), in particolare all'art. 1, comma 243, ha novellato l'art. 24-*bis* del d.l. 22 giugno 2012, n. 83, convertito con modificazioni dalla l. 7 agosto 2012, n. 134. Il mutamento della cornice normativa di riferimento – con particolare riguardo all'ampliamento del novero dei soggetti destinatari, delle informazioni che gli stessi sono tenuti a fornire e degli adempimenti che devono porre in essere – tocca in parte anche le attribuzioni già in passato rimesse al Garante e comporta la ridefinizione delle misure e degli adempimenti individuati con il provv. del 10 ottobre 2013, n. 444 (doc. web n. 2724806), successivamente integrato dal provv. 18 dicembre 2013, n. 582 (doc. web n. 2849324) i cui effetti sono stati caducati dalle previsioni contenute nel vigente art. 24-*bis*.

Già nella prima fase applicativa, le modifiche normative introdotte nonché la severità delle sanzioni previste hanno tuttavia sollevato alcune questioni interpretative portate all'attenzione dei soggetti menzionati dall'attuale art. 24-*bis*, comma 2, d.l. n. 83/2012 (segnatamente il Ministero dello sviluppo economico, il Ministero del lavoro, l'Autorità per le garanzie nelle comunicazioni e il Garante per la protezione dei dati personali), alle quali, a seguito di un esame comune, è stato fornito un primo riscontro, nelle "Domande frequenti (FAQ) in materia di *call center*" rese disponibili dal Ministero dello sviluppo economico sul proprio sito web (all'indirizzo http://www.sviluppoeconomico.gov.it/index.php/it/assistenza/domande-frequenti/2036069-*call-center*-domande-frequenti-faq) e, in relazione alle attribuzioni facenti specificatamente capo a ciascuno dei soggetti istituzionali, in più puntuali indicazioni impartite singolarmente. Anche l'Autorità, al fine di facilitare l'applicazione della nuova disciplina, ha così provveduto a redigere una prima nota informativa (doc. web n. 6029202) e ha predisposto due modelli (il cui contenuto è aggiornato rispetto a quello già reso disponibile con il provvedimento del 10 ottobre 2013, n. 444) volti ad agevolare l'assolvimento degli obblighi comunicativi diretti al Garante, adeguandone il contenuto alle sopravvenute disposizioni di legge, ed utilizzabili dagli operatori economici cui facciano capo le localizzazioni in Paesi terzi dell'attività di *call center*: un primo modello potrà essere utilizzato, ai sensi dell'art. 24-*bis*, comma 2, lett. *c*), da parte degli operatori economici che intendono localizzare l'attività di *call center* in Paesi terzi in tempi successivi all'entrata in vigore della nuova disciplina (doc. web n. 6030404); un secondo modello potrà invece essere utilizzato, ai sensi dell'art. 24-*bis*, comma 3, per gli operatori che abbiano localizzato l'attività di *call center* in Paesi terzi anteriormente all'entrata in vigore della nuova disciplina (doc. web n. 6030415).

In ossequio al principio di semplificazione (cfr. art. 12, comma 1, d.lgs. 7 marzo 2005, n. 82 del Cad), non dovranno tuttavia formare oggetto di comunicazione al Garante (e di successivo aggiornamento) le numerazioni telefoniche messe a disposizione del pubblico e utilizzate nell'attività delocalizzata di *call center* secondo quanto previsto dalla nuova cornice normativa. Al fine di evitare che gli operatori economici di cui all'art. 24-*bis*, comma 2, siano tenuti ad un duplice adempimento

di obblighi di comunicazione contenutisticamente identici concernenti le menzionate numerazioni telefoniche messe a disposizione del pubblico e utilizzate per i servizi delocalizzati di *call center*, con la conseguente duplicazione dei relativi archivi presso i soggetti destinatari, tali obblighi saranno quindi utilmente assolti, anche nei confronti del Garante (art. 24-*bis*, commi 2, lett. *c*) e 3, d.l. n. 83/2012), con la comunicazione delle informazioni previste dalla legge al Ministero dello sviluppo economico (art. 24-*bis*, comma 2, lett. *b*), d.l. n. 83/2012) e l'attestazione al Garante dell'adempimento degli stessi.

Per lo svolgimento dei compiti istituzionali rimessi al Garante (artt. 50, d.lgs. n. 82/2005 nonché 24-*bis*, d.l. n. 83/2012, come modificato, e 154 del Codice) e d'intesa con il Ministero dello sviluppo economico, oltre che con l'Autorità per le garanzie nelle comunicazioni, l'Autorità avrà accesso ai dati relativi alle numerazioni telefoniche oggetto di utilizzazione per svolgere i servizi delocalizzati di *call center* e ai dati identificativi dei soggetti che, ai sensi dell'art. 24-*bis*, commi 2, lett. *b*) e 11 d.l. n. 83/2012, li hanno trasmessi a detti Enti.

12 Propaganda elettorale

Con provvedimento 5 maggio 2016, n. 205 (doc. web n. 6358149) il Garante è tornato a pronunciarsi in merito all'utilizzo di dati personali per fini di propaganda elettorale attraverso il ricorso a modalità automatizzate di contatto, ribadendo che, nell'ambito di consultazioni elettorali, i candidati non possono usare a fini di propaganda elettorale i dati personali in loro possesso per ragioni istituzionali. Nel caso di specie il Garante ha quindi vietato ad un *ex* assessore di utilizzare l'indirizzario di posta elettronica (che non era pubblico, essendo ad esclusivo uso interno dell'amministrazione e nella sua disponibilità in virtù dell'incarico precedentemente ricoperto) in violazione del principio di finalità (essendo quella di propaganda non compatibile con quelle che ne avevano giustificato la raccolta). Sotto diverso profilo, peraltro, come affermato dal Garante in più occasioni, i partiti, le liste o i singoli candidati non possono utilizzare indirizzi di posta elettronica senza il consenso specifico e informato dei destinatari; consenso che, nel caso in esame, non è risultato acquisito, come pure non è risultato che i destinatari siano stati informati sull'uso che veniva fatto dei loro dati.

Ulteriori istruttorie sono in corso in relazione al trattamento di dati personali per finalità di propaganda politica, con particolare riferimento alle modalità di riscontro alle istanze di opposizione fatte valere dagli interessati.

13 Internet e dati personali *online*. Violazioni di dati personali nel settore delle comunicazioni elettroniche

Google

Nel corso dei 18 mesi concessi a Google per dare attuazione alle prescrizioni del 10 luglio 2014, n. 353 (doc. web n. 3283078), in conformità a quanto previsto da un apposito protocollo di verifica, l'Autorità ha ricevuto aggiornamenti trimestrali circa l'implementazione di una serie di misure a tutela degli utenti dei circa 70 servizi offerti. In particolare, a seguito degli interventi posti in essere, le informazioni fornite agli utenti sul trattamento dei loro dati sono più numerose e messe a disposizione in maniera più agevole. L'informativa esplicita ora le diverse finalità per le quali i dati sono raccolti e utilizzati, compresa la profilazione che prevede anche l'incrocio dei dati tra le diverse funzionalità offerte. L'informativa è stata resa più accessibile grazie a un *link* diretto che ne consente la visualizzazione con un solo "*click* di distanza" da ogni pagina del dominio. Sono state aggiunte inoltre informative per singoli prodotti e servizi ed inseriti *link* per agevolare i contatti con la società nonché predisposto un modulo per l'esercizio dei diritti da parte degli utenti. Google ha altresì implementato le misure per acquisire il consenso all'uso dei dati non solo per gli utenti autenticati, ma anche – sulla base di una specifica prescrizione del Garante – di quelli non autenticati; a questo proposito, è stato utilizzato un meccanismo che impone all'utente di effettuare necessariamente una scelta prevedendo, tramite la presentazione di un *banner*, la richiesta di consenso ripetuta per tre volte nell'arco di due mesi, fino a impedire l'accesso ai servizi finché la scelta non venga effettuata. Gli utenti potranno negare il consenso o rilasciarne uno, anche parziale, rispetto ai diversi scopi per i quali i dati possono essere usati, a partire dalla profilazione. Per la gestione dei propri dati personali, gli utenti autenticati (che cioè dispongono di un *account*) possono utilizzare un nuovo servizio denominato *My account* che contiene informazioni sulla *privacy*, la sicurezza e gli strumenti a disposizione per controllare i propri dati. Per gli utenti non autenticati è invece disponibile una versione semplificata che consente di personalizzare le ricerche sia sul motore di ricerca che su YouTube, controllare la tipologia di annunci visualizzati e scegliere di non ricevere pubblicità mirata. Migliorate anche le impostazioni degli annunci con la possibilità di selezionare le categorie di interesse o disattivare la pubblicità personalizzata. Infine, gli utenti possono ora sospendere la raccolta dei dati per la cronologia delle ricerche e delle localizzazioni o per l'attività vocale e audio. Come per la manifestazione del consenso, anche il diritto di opposizione al trattamento dei dati può essere esercitato in modo "granulare", cioè anche solo rispetto ad alcuni servizi e incroci di dati tra servizi diversi. Gli utenti avranno a disposizione un meccanismo di facile utilizzo per poter dialogare con Google ed esercitare i loro diritti, come chiedere copie dei dati o farli rettificare. In linea con quanto prescritto dal Garante, Google rende inaccessibili i dati dell'utente autenticato 24 ore dopo la richiesta dell'interessato e li cancella entro 2 mesi, se i dati sono su sistemi attivi, o entro 6 mesi, se sono archiviati su sistemi di *back up*. I cd. dati di sistema, necessari a Google per fornire i propri servizi (es. i *file* di *log*), vengono invece anonimizzati allo scadere di tempi di conservazione predefiniti. Con riferimento al tempo unico di conservazione indicato da Google per i *cookie* (18 mesi), l'Autorità si è riservata un ulteriore approfondimento per verificare se pos-

sano essere individuati tempi di conservazione diversificati in base al maggiore o minore potere identificativo dei *cookie*; così pure rispetto alle tecniche di anonimizzazione utilizzate.

"Ricerca inversa" *online*

A seguito di numerose segnalazioni con le quali si è lamentata la diffusione su un sito web di un elenco di utenze telefoniche (in assenza di consenso da parte degli interessati) e all'esito delle verifiche risultate, non provenienti dal DBU (*Data base* unico), ma acquisite in maniera automatica e indiscriminata attraverso *script* "lanciati" direttamente sulle fonti web (cd. web *scraping*), che consentivano la consultabilità *online* delle numerazioni (anche "riservate") e la "ricerca inversa" delle generalità dei contraenti, con il provvedimento 14 gennaio 2016, n. 4 (doc. web n. 6053915) se ne è vietata l'ulteriore diffusione. Con detta decisione il Garante, evidenziando che non è legittimo formare un elenco telefonico, *online* o anche cartaceo, con dati che non siano tratti dalla base di dati unica degli operatori di comunicazione elettronica (DBU) già previsto dalla delibera Agcom n. 36/02/CONS, e che non è consentita, tramite la consultabilità di tale elenco, la funzione di cd. ricerca inversa (ossia la ricerca delle generalità dei contraenti, sulla base del loro numero telefonico, senza aver previamente acquisito il loro consenso libero e specifico, oltre che informato), ha ordinato la cancellazione di detto *database*.

WhatsApp/Facebook

Il 25 agosto 2016 WhatsApp Inc. – società del gruppo Facebook Inc. dal 2014 – ha modificato le regole contenute nei "termini e informativa sulla *privacy*" in relazione ai propri servizi di messaggistica rendendo pubblici, tramite il proprio *blog* https://blog.whatsapp.com, i termini essenziali dell'operazione. In prima approssimazione, l'effetto di detta modifica sarebbe quello di mettere a disposizione di Facebook le informazioni concernenti i singoli *account* WhatsApp. Nei confronti degli interessati le modifiche introdotte sono state illustrate al momento dell'attivazione dell'applicazione per usufruire del servizio sui singoli *device*, schiudendosi per l'utente, in tale occasione, due opzioni: accettare immediatamente, sostanzialmente "a scatola chiusa", le nuove condizioni (con l'effetto che le informazioni relative all'*account* raccolte da WhatsApp vengano condivise con Facebook) ovvero, mediante opportune operazioni effettuate sul *device*, optare per la soluzione di non condividere *chat* e numero di telefono su Facebook.

Rispetto a tali complessive operazioni, l'Autorità – procedendo d'intesa con altre autorità europee di protezione dei dati – ha formulato una richiesta di informazioni nei confronti delle società coinvolte al fine di verificare la complessiva correttezza dei trattamenti effettuati; i riscontri forniti sono, allo stato, in fase di valutazione.

IoT

Dopo aver avviato con provvedimento 26 marzo 2015, n. 179 (doc. web n. 3898704) una consultazione pubblica sul cd. Internet delle Cose (*Internet of Things* - IoT) – preordinata all'individuazione, allo stato dell'arte, dei rischi per la protezione dei dati personali connessi dall'impiego di tecnologie che consentono l'interconnessione (e l'interazione) di oggetti e sistemi diversi (*smartphone*, *tablet* e pc, ma anche oggetti di uso quotidiano come, tra gli altri, dispositivi indossabili, di automazione domestica, di geolocalizzazione e navigazione assistita) – l'Autorità ha continuato a seguire gli sviluppi in materia, anche partecipando, nell'ambito del *Global Privacy Enforcement Network* (GPEN), all'iniziativa (*Privacy Sweep*), svoltasi nel 2016, dedicata all'IoT: anche se il fenomeno non sembra aver assunto ancora una dimensione di mercato, con riferimento a non poche applicazioni si è riscontrato uno scarso livello di trasparenza circa il trattamento di dati personali, anche sensibili, che tali dispositivi consentono e criticità in punto di sicurezza (cfr. 24.3).

Data breach

Confermando la tendenza rilevata nell'anno precedente, nel 2016 sono pervenute 43 comunicazioni di violazioni di dati personali da parte dei più importanti fornitori di servizi di comunicazione elettronica stabiliti sul territorio nazionale.

La maggior parte delle violazioni notificate ha riguardato l'accesso non autorizzato ai dati personali che, nella quasi totalità dei casi, ha riguardato eventi che, in base a quanto rappresentato, hanno coinvolto un numero limitato di interessati (inferiore a cento).

Tra le istruttorie condotte, merita di essere segnalato un approfondito accertamento *in loco* effettuato dall'Ufficio sulla base di un articolato reclamo – nel quale si lamentava l'erronea attribuzione di centinaia di utenze telefoniche e l'indebita azione di recupero del credito per asseriti mancati pagamenti riferiti a talune di dette utenze – nei confronti di un primario gestore di telefonia i cui esiti sono, allo stato, oggetto di valutazione.

14 La protezione dei dati personali nell'ambito del rapporto di lavoro pubblico e privato

Com'è noto nel 2015 è stata completata la cd. riforma del lavoro (o *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 di dati personali, sia sotto il profilo del trattamento di informazioni in grandi banche dati nel settore lavoristico (anche di nuova istituzione e nell'ambito del sistema informativo unitario delle politiche del lavoro; d.lgs. nn. 150/2015 e 151/2015), sia per quanto riguarda la disciplina dei controlli a distanza dell'attività dei lavoratori (art 23, d.lgs. n. 151/2015 che ha modificato l'art. 4, l. n. 300/1970, recante lo Statuto dei lavoratori) (cfr. Relazione 2015, par. 2.1.2). Il Garante aveva seguìto l'*iter* di approvazione di tali atti normativi formulando anche osservazioni critiche nel corso dell'esame parlamentare degli schemi di decreto, in due audizioni presso le Commissioni lavoro della Camera e del Senato (tenute rispettivamente il 9 e il 14 luglio 2015, doc. web n. 4119045).

Nel 2016 sono stati portati all'attenzione dell'Autorità diversi trattamenti effettuati in tale ambito rispetto ai quali ha trovato applicazione la nuova disciplina dei controlli a distanza, nell'esame dei quali il Garante ha avuto modo di affrontare alcuni aspetti meritevoli di attenzione sul piano interpretativo ed applicativo. In particolare, come meglio si vedrà avanti (cfr. par. 14.2), un provvedimento del Garante ha rappresentato la prima occasione in cui l'Autorità ha espresso il proprio orientamento sull'ambito di applicazione del comma 2 del predetto art. 4 dello Statuto dei lavoratori come modificato dal citato art. 23, d.lgs. n.151/2015, 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.

Il Garante è altresì intervenuto in merito al trattamento di dati biometrici dei lavoratori per finalità di sicurezza o di rilevazione delle presenze nel quadro della più generale esigenza di assicurare il rispetto dell'obbligo di prestazione lavorativa a fronte di casi di assenteismo verificatisi in alcune amministrazioni pubbliche (cfr. par. 16.2).

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. 14.4), o in caso di pubblicazione dei dati dei lavoratori, anche in relazione alle possibili interferenze con la disciplina in materia di trasparenza (cfr. par. 14.3).

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

Con riferimento ai trattamenti di dati personali effettuati attraverso sistemi che consentono la localizzazione geografica dei dipendenti nell'ambito del rapporto di lavoro, anche nel 2016 si registra un incremento dei casi sottoposti all'attenzione dell'Autorità sia con segnalazioni, sia con istanze di verifica preliminare presentate dai titolari del trattamento, sia all'esito di attività di controllo effettuate anche con accertamenti *in loco*.

Tale incremento è indice dell'uso sempre più diffuso di dispositivi tecnologici completi di funzionalità di geolocalizzazione nel contesto dei processi produttivi, preordinati al raggiungimento di finalità eterogenee.

In materia il Garante ha adottato un provvedimento di carattere generale relativo alla geolocalizzazione di veicoli (cfr. provv. 4 ottobre 2011, n. 370, doc. web n. 1850581), nonché due provvedimenti "pilota" relativi all'utilizzo di applicazioni informatiche che consentono di localizzare geograficamente dispositivi mobili (*smartphone*) forniti in dotazione ai dipendenti (cfr. provv.ti 11 settembre 2014, n. 401, doc. web n. 3474069 e 9 ottobre 2014, n. 448, doc. web n. 3505371). L'Autorità ha in particolare ritenuto che il trattamento di dati personali riferiti alla localizzazione di dispositivi – che, differentemente dai veicoli di servizio, da un lato "seguono" costantemente il dipendente, dall'altro si prestano comunemente ad utilizzi anche privati, spesso consentiti dal datore di lavoro – presenta rischi specifici per le libertà (es. di circolazione e di comunicazione), i diritti e la dignità dei lavoratori.

In relazione a tali trattamenti, inoltre, il Garante ha rammentato che la localizzazione dei dati relativi alla posizione geografica è soggetta all'obbligo di notificazione ai sensi dell'art. 37, comma 1, lett. *a*) del Codice.

Per quanto riguarda l'applicazione ai predetti sistemi della disciplina in materia di controlli a distanza dell'attività del lavoratore (art. 4, l. 20 maggio 1970, n. 300, recante lo Statuto dei lavoratori, richiamato dall'art. 114 del Codice), si segnala che a seguito delle recenti modifiche apportate al citato art. 4 dal d.lgs. 14 settembre 2015, n. 151 (art. 23), l'Ispettorato nazionale del lavoro, con circolare n. 2 del 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 da parte dell'Ispettorato nazionale del lavoro".

Uso delle tecnologie di geolocalizzazione per finalità di rilevazione delle presenze

Il Garante, nell'ambito di un procedimento di verifica preliminare, ha ammesso l'utilizzo di un sistema di rilevazione di inizio e fine dell'attività lavorativa (e della pausa pranzo, se prevista) prospettato da due società operanti nel settore dell'intermediazione in materia di lavoro. Il sistema prospettato – ferma restando l'alternatività con gli altri strumenti già in uso e rimasti comunque a disposizione – si basava sull'installazione sui dispositivi *smartphone* di proprietà dei lavoratori di un applicativo sviluppato da un soggetto terzo designato responsabile del trattamento.

Considerato che la gran parte dei dipendenti svolgeva la propria attività lavorativa al di fuori della sede aziendale, sia presso l'utilizzatore (in caso di somministrazione di lavoro) sia presso i clienti, il sistema sottoposto a verifica preliminare avrebbe consentito alle società richiedenti di realizzare risparmi di gestione nonché di semplificare e di incrementare l'efficienza e la certezza dell'attività di rilevazione delle presenze, anche a favore dell'effettiva certificazione delle ore lavorate presso l'utilizzatore.

L'Autorità, nella prospettiva della *privacy by design*, ha impartito alcune misure a tutela dei diritti degli interessati, in attuazione del principio di necessità (art. 3 del Codice). In particolare, considerata l'incidenza di errori nella rilevazione della posizione geografica (dovuti sia al sistema che ai GPS installati sui singoli dispositivi mobili) e rilevata la diversità dell'informazione raccolta rispetto ai sistemi ordinari di rilevazione delle presenze, il Garante ha stabilito che le società dovranno configurare il sistema in modo da cancellare le coordinate geografiche della posizione del lavoratore, dopo aver verificato preventivamente – al fine di scongiurare abusi – l'associazione tra le coordinate geografiche della sede di lavoro e la posizione del lavo-

14

ratore, e conservando eventualmente il solo dato relativo alla sede di lavoro, oltre che la data e l'orario cui si riferisce la "timbratura". Il sistema inoltre dovrà rendere sempre visibile un'icona che indichi che la funzionalità di localizzazione è attiva. Deve altresì essere preventivamente impedito il trattamento anche accidentale di dati presenti sul dispositivo riferiti alla vita privata del lavoratore (dati relativi al traffico telefonico, agli sms, alla posta elettronica, alla navigazione in internet ed altro) (provv. 8 settembre 2016, n. 350, doc. web n. 5497522).

Sistemi di localizzazione dei dispositivi affidati al personale in servizio all'esterno

In un altro caso l'Autorità ha ritenuto conforme ai princìpi di protezione dei dati l'adozione di un sistema basato sull'installazione di un'applicazione – contenente una funzionalità di localizzazione – sugli *smartphone* forniti in dotazione ai dipendenti impegnati all'esterno della sede aziendale. Il sistema era configurato per rilevare, a seguito dell'attivazione di apposito pulsante, l'orario e il luogo di "inizio e fine lavoro", "inizio pausa pranzo" e "inizio e fine di evento meteorologico di maltempo". Anche in questo caso l'applicazione era sviluppata da un soggetto terzo che però non aveva accesso ai dati raccolti.

Il Garante ha ritenuto lecito lo scopo prefisso, vale a dire la possibilità di effettuare con modalità automatiche (conformemente a quanto previsto dal contratto) il calcolo delle indennità di viaggio e trasferta o altri emolumenti, commisurato al luogo in cui l'attività lavorativa è stata effettuata oppure di acquisire elementi preordinati alla presentazione all'ente competente delle domande di cassa integrazione per impossibilità di svolgere la prestazione lavorativa in caso di particolari eventi meteorologici. Il trattamento è stato ritenuto lecito anche considerato che la società titolare del trattamento, in attuazione del cit. art. 4 dello Statuto dei lavoratori, ha stipulato un accordo con le rappresentanze sindacali. Sono state altresì ritenute conformi al principio di proporzionalità, pertinenza e non eccedenza la disattivazione del dispositivo al di fuori dell'orario di lavoro e nella pausa pranzo e la predisposizione del sistema in modo da non consentire la localizzazione geografica dei dispositivi al di fuori dei casi stabiliti.

Anche in questo caso sono state impartite misure ed accorgimenti a tutela degli interessati, come la necessità di configurare il sistema in modo da impedire il trattamento di dati ulteriori e non pertinenti rispetto alle finalità indicate (in particolare dei dati relativi al traffico telefonico, agli sms, alla posta elettronica, alla navigazione in internet). Il sistema deve altresì prevedere, anche quando l'applicazione lavora in *background*, la presenza di un'icona che indichi che la funzionalità di localizzazione è attiva (provv. 18 maggio 2016, n. 226, doc. web n. 5217175).

Uso di sistemi di localizzazione all'interno di una cd. scatola nera

Conformemente a quanto già deciso in casi analoghi (cfr. provv. 29 novembre 2012, n. 368, doc. web n. 2257616), il Garante in sede di verifica preliminare ha ammesso l'installazione di un dispositivo a bordo di veicoli che svolgono il servizio di trasporto pubblico locale, in grado di raccogliere una pluralità di dati quali la localizzazione geografica del veicolo, immagini mediante un sistema di videoregistrazione nonché alcuni altri dati quali la velocità, le accelerazioni e decelerazioni improvvise. I dati raccolti sono memorizzati per 72 ore (il tempo necessario ad effettuare le necessarie verifiche) ed eventualmente conservati solo in caso di eventi ritenuti rilevanti ossia i sinistri o l'attivazione del sistema di allarme da parte dell'autista, limitatamente ad un contenuto ambito temporale (20 secondi), immediatamente precedente e successivo al verificarsi dell'evento.

Nella descrizione della società richiedente le finalità del sistema consistevano nella ricostruzione della dinamica dei sinistri, nel rafforzamento della sicurezza di dipendenti, utenti e beni aziendali nonché nella razionalizzazione del servizio prestato, considerato che – sotto quest'ultimo profilo – il sistema avrebbe consentito di visualizzare gli itinerari percorsi dai mezzi.

Le finalità perseguite dal titolare con l'installazione del descritto sistema sono state ritenute dall'Autorità lecite, considerato anche che in applicazione dell'art. 4 dello Statuto, è stato raggiunto un accordo con le rappresentanze sindacali.

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, misure tecniche idonee a non consentire l'identificazione di soggetti non coinvolti nei sinistri o negli altri eventi rilevanti in caso di comunicazione a terzi dei dati raccolti e ad anonimizzare – con contestuale adozione di modalità di utilizzo in forma aggregata – i dati relativi alla localizzazione geografica trattati allo scopo di razionalizzare il servizio di trasporto prestato (provv. 25 febbraio 2016, n. 78, doc. web n. 4807812).

14.2. *Il trattamento di dati personali dei dipendenti mediante dispositivi e posta elettronica*

Software di gestione dei servizi di rete e "strumenti di lavoro"

L'utilizzo dei servizi di comunicazione elettronica (internet, posta elettronica aziendale) – già oggetto, in termini generali, di specifiche linee guida del Garante (provv. 1° marzo 2007, linee guida per posta elettronica e internet, doc. web n. 1387522) – ha formato oggetto di verifica in relazione al trattamento posto in essere da un Ateneo italiano e avente ad oggetto *file* di *log*, MAC *Address (Media Access Control Address*), indirizzo IP nonché altre informazioni relative all'accesso ai servizi internet, alla posta elettronica e alle connessioni di rete, da parte di una pluralità di utenti (personale tecnico amministrativo, docenti, ricercatori e studenti). Tali informazioni, raccolte e conservate per un periodo di 5 anni, erano oggetto di ulteriori operazioni di trattamento per il tramite degli amministratori di sistema, quali, il monitoraggio e il filtraggio delle stesse. Contrariamente a quanto sostenuto dall'Ateneo, l'accertamento ha evidenziato che i dati raccolti erano chiaramente riconducibili ai singoli utenti, anche grazie al tracciamento puntuale degli indirizzi IP e dei MAC *Address* (identificativo *hardware*) dei computer assegnati ai dipendenti o in uso agli altri utenti abilitati, consentendo di risalire, anche indirettamente, alla postazione corrispondente e, quindi, all'utente che vi operava (cfr., Gruppo Art. 29, parere n. 4/2007 – WP 136 sul concetto di dato personale; sul carattere di dato personale del MAC *Address* stante la relativa univocità, cfr. Gruppo Art. 29, parere n. 13/2011 – WP 185 sui servizi di geolocalizzazione su dispositivi mobili intelligenti, spec. p. 11).

All'esito dell'accertamento l'Autorità ha dichiarato illecito il trattamento, con la conseguente inutilizzabilità dei dati trattati in violazione di legge (art. 11, comma 2 del Codice) e disposto il divieto dell'ulteriore trattamento su base individuale dei dati personali, salva la conservazione di quelli necessari ai fini della eventuale acquisizione da parte dell'autorità giudiziaria.

Il trattamento effettuato dall'Ateneo infatti è stato ritenuto in contrasto con i princìpi di necessità, pertinenza e non eccedenza (artt. 3 e 11, comma 1, lett. *a*) e *d*) del Codice) che non consentono controlli massivi, prolungati e indiscriminati, ma impongono di privilegiare soluzioni ispirate alla gradualità del monitoraggio e alla residualità di controlli. L'Ateneo non aveva poi reso la dovuta informativa in favore degli utilizzatori della rete, anche con riguardo alle effettive caratteristiche delle operazioni di trattamento effettuate (art. 13 del Codice), né a tal fine è risultato idoneo il regolamento interno sull'utilizzo degli strumenti elettronici.

Il descritto sistema era stato inoltre configurato con funzionalità tali da permettere operazioni di controllo dell'attività e dell'utilizzo dei servizi della rete effettuato da soggetti identificabili. Sotto questo profilo è stato accertato che il trattamento nei

14

confronti dei dipendenti dell'Ateneo era effettuato in violazione anche della disciplina sull'impiego di apparecchiature idonee al controllo a distanza dell'attività dei lavoratori (art. 4, l. n. 300/1970 e art. 114 del Codice).

Sotto quest'ultimo profilo, il provvedimento del Garante ha rappresentato la prima occasione in cui l'Autorità ha espresso il proprio orientamento sull'ambito di applicazione del comma 2 del citato art. 4 della l. n. 300/1970 quale risultante dalle modifiche intervenute per effetto dell'art. 23, d.lgs. n. 151/2015 (riforma del lavoro o *Jobs act*), 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 (la procedura di "concertazione" sindacale o l'equivalente autorizzazione dell'organo pubblico di controllo).

Il Garante, infatti (con ciò muovendosi nel solco di quanto già tracciato, seppure in termini più generali, dal Ministero del lavoro delle politiche sociali, con nota 18 giugno 2015), ha precisato che – con riferimento agli strumenti oggetto del provvedimento, vale a dire servizio di posta elettronica e navigazione web – possono ritenersi ricompresi nella predetta nozione solo "servizi, *software* o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza". A titolo esemplificativo, possono essere considerati "strumenti di lavoro" alla stregua della normativa sopra citata il servizio di posta elettronica offerto ai dipendenti (mediante attribuzione di un *account* personale) e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore (ad es., sistemi di *logging* per il corretto esercizio del servizio di posta elettronica, con conservazione dei soli dati esteriori, contenuti nella cd. *envelope* del messaggio, per una breve durata non superiore comunque ai sette giorni; sistemi di filtraggio anti-*virus* che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui *server* per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso).

Viceversa – ha concluso coerentemente il Garante- non possono considerarsi "strumenti di lavoro" nei termini anzidetti *software* che consentano, con modalità indipendenti e non percepibili dall'utente (cd. in *background*) e senza alcun impatto o interferenza sulla normale attività dell'utilizzatore, costanti operazioni di "monitoraggio", "filtraggio", "controllo" e "tracciatura" degli accessi a internet o al servizio di posta elettronica (provv. 13 luglio 2016, n. 303, doc. web n. 5408460).

Controlli sulla posta elettronica aziendale e su dispositivi *Blackberry* affidati ai dipendenti

All'esito di un procedimento seguito alla proposizione di un reclamo, il Garante ha disposto il divieto dei trattamenti di dati personali dei dipendenti effettuato da una società attraverso il servizio di posta elettronica aziendale (sia in costanza del rapporto di lavoro che successivamente alla sua interruzione) e tramite l'utilizzo dei dispositivi *Blackberry* affidati in dotazione ai dipendenti.

In particolare, l'Autorità ha ritenuto illecita la sistematica conservazione sul *server* aziendale dei dati esterni e dei contenuti delle comunicazioni elettroniche effettuate attraverso gli *account* di posta elettronica aziendali, peraltro per un periodo di tempo – dieci anni – ritenuto non conforme ai princìpi di necessità, pertinenza e non eccedenza in quanto non commisurato alle ordinarie necessità di gestione dei servizi di posta elettronica ivi comprese quelle di sicurezza dei sistemi. Tali dati, gestiti anche da un soggetto terzo in assenza di idoneo criterio di legittimazione, erano accessibili alla società nell'ambito di una procedura di *security investigation request*. È emerso che tale complessiva attività non era stata in alcun modo resa nota ai dipendenti, né attraverso informative individualizzate né tramite i documenti

relativi alle politiche aziendali in materia di utilizzo degli strumenti informatici, in contrasto con l'obbligo per il datore di lavoro di fornire una previa informativa ai dipendenti su tutti i trattamenti effettuati, anche in base al principio di correttezza. Inoltre tale trattamento consentiva alla società di effettuare il controllo dell'attività dei dipendenti in violazione della disciplina di settore (cfr. artt. 11, comma 1, lett. *a*) e 114 del Codice nonché art. 4, l. n. 300/1970). Tale disciplina, pure a seguito delle modifiche introdotte con il già citato articolo 23 del d.lgs. n. 151/2015, non consente l'effettuazione di attività idonee a realizzare (anche indirettamente) il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore (v. linee guida per posta elettronica e internet, provv. 1° marzo 2007, n. 13, doc. web n. 1387522, spec. par. 4, 5.2. lett. *b*) e 6; si veda anche Consiglio di Europa, raccomandazione del 1° aprile 2015, CM/Rec(2015)5, spec. princ. 14). Inoltre, posto che la società permetteva – ragionevolmente – l'uso di *e-mail* a scopo privato, tali operazioni avrebbero consentito l'eventuale trattamento di dati "non rilevanti ai fini della valutazione dell'attitudine professionale" del dipendente nonché di dati sensibili, in violazione dell'art. 8 dello Statuto dei lavoratori e 10 del d.lgs. n. 276/2003.

È stata altresì ritenuta non conforme alle disposizioni in materia di protezione dei dati personali la procedura adottata dalla società consistente nel mantenere attive fino a sei mesi le caselle di posta elettronica aziendale dopo la cessazione del rapporto di lavoro. In base all'orientamento consolidato dell'Autorità, dopo la cessazione del rapporto gli *account* riconducibili a persone identificate o identificabili devono essere rimossi previa disattivazione degli stessi e contestuale adozione di meccanismi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del datore di lavoro (v. da ultimo provv. 30 luglio 2015, n. 456, doc. web n. 4298277).

Per quanto riguarda l'utilizzo dei dispositivi *Blackberry* è stata ritenuta illecita la possibilità per la società di accedere da remoto ai contenuti (anche di natura privata) presenti nel dispositivo nonché di raccogliere, conservare, comunicare a terzi e cancellare i dati. Ciò pur in presenza di un'informativa (che peraltro non menzionava la presenza di un'applicazione in grado di rilevare le soglie di consumo di ciascun utente), in quanto le descritte attività sono state ritenute non conformi ai princìpi di liceità (anche con riferimento ai già menzionati artt. 4 e 8, l. n. 300/1970 richiamati dagli artt. 113 e 114 del Codice), necessità, pertinenza e non eccedenza.

Il Garante ha infine invitato la società ad adottare di regola – a seguito dell'interruzione del rapporto di lavoro o di trasferimento del dipendente – procedure che consentano a quest'ultimo di partecipare alla ricognizione e, se del caso, alla consegna di documenti o di oggetti collocati all'interno degli uffici, soprattutto in caso di assegnazione individuale di spazi e postazioni (provv. 22 dicembre 2016, n. 547, doc. web n. 5958296).

14.3. *Pubblicità e trasparenza dei dati dei lavoratori*

Pubblicazione *online* di dati idonei a rivelare la condizione di disabilità

Nonostante la pregressa attività di sensibilizzazione del Garante, continuano a pervenire segnalazioni e notizie in tema di pubblicazione *online* sui siti istituzionali degli enti pubblici di dati, atti o provvedimenti contenenti dati personali riferiti a lavoratori. Il tema già oggetto di precedenti pronunce è stato nuovamente affrontato nel 2016 con specifico riguardo alla diffusione dei dati idonei a rivelare la condizione di disabilità o comunque idonee a rivelare lo stato di salute di lavoratori o partecipanti alle prove concorsuali, a volte nell'ambito di procedure selettive "riservate" ai sensi della l. n. 68/1999. Nella maggior parte dei casi, i dati erano conte-

nuti in graduatorie o altri atti, reperibili in rete tramite motori di ricerca generalisti, che recavano in chiaro i dati identificativi delle persone. In applicazione dell'art. 22, comma 8, del Codice, a seguito delle necessarie verifiche, è stata dichiarata l'illiceità della diffusione di dati sulla salute dei soggetti interessati analogamente a qualsiasi riferimento alla condizioni di invalidità, disabilità o handicap fisici e/o psichici – in qualche caso anche altre informazioni eccedenti (ad es., il codice fiscale) – disponendo il divieto dell'ulteriore diffusione in internet e prescrivendo ai titolari del trattamento (in prevalenza province e comuni) l'adozione di idonei accorgimenti nelle operazioni di trattamento funzionali alla pubblicazione di tali atti e attivando i conseguenti procedimenti sanzionatori sul piano amministrativo (cfr., anche, linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati, adottate con provv. 15 maggio 2014, n. 243, doc. web n. 3134436, parte II, punti 1 e 3.b.) (provv. ti 4 febbraio 2016, nn. 35 e 36, doc. web nn. 4727305 e 4912481; provv. 1° giugno 2016, n. 244, doc. web n. 5260571).

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

Trattamento di dati giudiziari di personale operante nei contesti educativi

Nel corso dell'anno il Garante si è pronunciato su trattamenti di dati personali nella gestione del rapporto di lavoro, affrontando in particolare il tema del trattamento di dati giudiziari del personale da parte del datore di lavoro al fine di accertare il possesso di requisiti dei dipendenti per l'accesso a particolari impieghi o mansioni; ciò con riguardo ad una società di gestione di asili nido che aveva chiesto, anche in vista di future assunzioni, di poter essere autorizzata ad acquisire in via periodica (con cadenza biennale) il certificato penale del casellario ed il certificato dei carichi pendenti degli interessati. Nel caso esaminato il Garante non ha ritenuto sussistenti i presupposti per autorizzare, ai sensi dell'art. 41 del Codice, il trattamento dei dati giudiziari dei dipendenti a contatto con i minori (educatori, coordinatori, cuochi ed ausiliari) presso gli asili nido gestiti dalla società istante.

Premesso che in base alla disciplina in materia di protezione dei dati personali, i soggetti privati possono trattare i dati giudiziari soltanto se autorizzati da espressa disposizione di legge o da provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (art. 27 del Codice), il Garante non ha ritenuto sussistenti i presupposti per emanare un'autorizzazione specifica nei confronti della società richiedente. La materia è infatti disciplinata dall'art. 25-*bis*, d.P.R. 14 novembre 2002, n. 313 (disposizione introdotta dall'art. 2, d.lgs. 4 marzo 2014, n. 39, in attuazione della direttiva 2011/93/UE, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, ma v. già, decisione quadro 2004/68/GAI) che ha stabilito presupposti, limiti e condizioni, sul piano oggettivo e soggettivo, per l'acquisizione del pertinente certificato del casellario giudiziale da parte di chi intenda impiegare una persona per lo svolgimento di attività professionali che comportino contatti diretti e regolari con minori, al fine di verificare l'esistenza di condanne per fattispecie di reati indicate tassativamente dalla legge (sul punto, Ministero della giustizia, circolari 3 aprile 2014 e 24 luglio 2014 e note di chiarimento disponibili su www.giustizia.it; Ministero del lavoro e delle politiche sociali, circolare n. 9 dell'11 aprile 2014 e interpelli n. 25 del 15 settembre 2014 e n. 22 del 24 settembre 2015 nonché nota del 13 gennaio 2016, prot. 29/0000115/P).

Nel corso dell'istruttoria non sono state peraltro rappresentate, né sono emerse, circostanze particolari o situazioni eccezionali tali da consentire un trattamento difforme o ulteriore rispetto a quanto previsto dalla normativa di settore e da quanto già consentito dall'autorizzazione generale del Garante n. 7 (con riguardo al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici), né è stato ritenuto ammissibile individuare, in contrasto con la normativa vigente, ipotesi di accesso diretto ai predetti dati giudiziari non previste dalla citata disciplina in materia di casellario giudiziale (d.P.R. n. 313/2002) (provv. 15 dicembre 2016, n. 533, doc. web n. 5971199).

14.5. *Il trattamento di dati sulla salute del personale navigante da parte del "medico competente" del vettore aereo*

Nel corso dell'anno di riferimento il Garante, nell'esprimere il proprio avviso su un quesito del Ministero della salute, ha approfondito, per i profili di più diretto impatto sulla disciplina di protezione dei dati, la materia dei livelli di sicurezza del traffico aereo, anche alla luce del quadro normativo sovranazionale. Il Garante ha espresso il proprio avviso sul tema della comunicazione al medico competente di un vettore aereo nell'ambito dello svolgimento dei propri compiti in materia di igiene e sicurezza del lavoro (cd. sorveglianza sanitaria, art. 41, d.lgs. n. 81/2008), di dati relativi alla salute del personale navigante legittimamente trattati nell'ambito del procedimento per il rilascio delle licenze aeronautiche per l'aviazione civile dai soggetti pubblici istituzionalmente preposti alla verifica dei requisiti psico-fisici (AeMC, *aeronautical medical centre* che in Italia sono svolte dai competenti uffici dell'Aeronautica militare -IMAS e del Ministero della salute - SASN). Il Dicastero aveva formulato una richiesta circa la liceità della messa a disposizione in favore del medico competente operante presso un vettore aereo di documentazione sanitaria contenente informazioni relative alle limitazioni della licenza di volo dei piloti (segnatamente "il giudizio di non idoneità o di limitazione dell'idoneità al volo e ai privilegi della licenza"). Lo studio è stato condotto anche alla luce dei riscontri fatti pervenire dagli altri Stati membri interpellati sul tema e dei contributi tecnici di organismi che operano nel settore dell'aviazione civile a livello europeo (EASA, *Task force on measures following the accident of German Wings flight 9525- Final repor*t; EASA, *Action plan for the implementation of the Germanwings Task Force recommendations*. *Version 1 – 7 October* 2015; BEA, *Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, Rapport Final, Accident survenu le 24 mars 2015à Prads-Haute-Bléone (04) à l'Airbus A320-211, immatriculé D-AIPXexploité par Germanwings*- 13 marzo 2016).

A seguito di una valutazione del complessivo trattamento prospettato alla luce dell'articolata normativa che disciplina la materia sotto il profilo dell'accrescimento dei livelli di sicurezza del traffico aereo, è emerso che il quadro normativo di riferimento consentirebbe ai Servizi assistenza sanitaria ai naviganti (SANS) del Ministero della salute di comunicare gli esiti delle visite mediche - da loro effettuate in qualità di AeMC - all'Enac, in qualità di "autorità competente" e organo di controllo del settore aeronautico sotto la vigilanza dell'EASA (*European Aviation Safety Agency*), non invece ai datori di lavoro operanti nel settore della aeronavigazione (regolamento (UE) n. 290/2012, Allegato IV, ARA.MED.150 e regolamento Enac "Organizzazione sanitaria e certificazioni mediche d'idoneità per il conseguimento delle licenze e degli attestati aeronautici" Edizione 3-4 maggio 2015).

Al trattamento dei dati idonei a rivelare lo stato di salute delle persone (art. 4,

14

comma 1, lett. *d*), del Codice) trovano anzitutto applicazione gli artt. 3, 11, 20 e, con specifico riguardo al trattamento da parte di soggetti privati, l'art. 26 del Codice e dall'autorizzazione generale del Garante n. 1, con riguardo ai trattamenti strettamente correlati all'adempimento di specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria connessi alla gestione del rapporto di lavoro ivi compresi quelli in materia di igiene e sicurezza del lavoro (artt. 25 e 41 ss, d.lgs. n. 81/2008, cit.; autorizzazione generale n. 1 punto 1, lett. *c*), punto 3 e punto 4, lett. *c*).

In tale quadro il Garante ha ritenuto che le finalità di tutela della sicurezza dei voli e della salvaguardia della vita e dell'incolumità della collettività rispondano ad un interesse pubblico rilevante al quale concorrono sia gli accertamenti sanitari, a carico del Ssn, necessari per il rilascio delle licenze nell'ambito del sistema pubblicistico di verifica dell'idoneità al volo dei piloti o aspiranti tali, sia gli adempimenti di sorveglianza sanitaria, obbligatoriamente posti in essere dal datore di lavoro per il tramite del medico competente, volti a verificare l'idoneità del pilota alla "*mansione specifica*" (artt. 11, comma 1 lett. *a*) e *b*), 20, comma 1, e 85, comma 1, lett. *a*), *d*) ed *e*), del Codice; regolamento (UE) n. 1178/2011; d.lgs. 25 luglio 1997, n. 250, istitutivo dell'Enac). Tuttavia il Garante ha precisato che allo stato della normativa vigente, non risulta ammissibile un flusso di dati sanitari dei piloti dai competenti organismi pubblici in favore del medico operante presso i vettori aerei, né la consultazione da parte dello stesso delle medesime informazioni eventualmente disponibili in banche dati. Nel richiamare l'attenzione sull'opportunità di integrare il quadro normativo vigente, il Garante si è riservato la facoltà di esprimere le valutazioni di competenza sulle eventuali future disposizioni regolamentari (artt. 20, comma 2 e 154, commi 1, lett. *g*), e 4 del Codice) (provv. 27 aprile 2016, n. 194, doc. web n. 5149198).

15 Le attività economiche

15.1. *Il settore bancario*

Nel corso del 2016 un elevato afflusso di istanze (quesiti, richieste di parere, segnalazioni e reclami) ha impegnato l'attività del Garante su profili già affrontati e definiti in numerosi provvedimenti, incluse le linee guida adottate il 25 ottobre 2007 in materia di trattamenti di dati personali effettuati da banche nei rapporti con la clientela (doc. web n. 1457247). Molteplici, quindi, sono stati i riscontri resi a specifici interessati sui temi della comunicazione a terzi di dati inerenti clienti nonché sull'esercizio del diritto di accesso ai dati di congiunti deceduti relativi a rapporti bancari. Altre risposte hanno riguardato, invece, quesiti concernenti le corrette modalità di richiesta e manifestazione del consenso al trattamento dei dati personali a fini di informazione commerciale, offerte dirette, indagini di mercato o *customer satisfaction* (concernenti prodotti e servizi offerti da alcune banche), o riguardanti lo svolgimento di attività di profilazione della clientela.

Circolazione delle informazioni e tracciamento delle operazioni bancarie

Al fine di valutare lo stato di implementazione delle prescrizioni contenute nel provvedimento generale adottato il 12 maggio 2011 e divenuto pienamente efficace il 1° ottobre 2014, recante prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie, è stato effettuato un articolato ciclo di accertamenti ispettivi disposti d'ufficio, iniziati già nel 2015 e proseguiti nel 2016, su un significativo campione di istituti di credito, rappresentati sia da ABI che da Federcasse.

Tale attività ha evidenziato che, pur se con differenze, dovute alle distinte strutture organizzative e ai diversi sistemi informatici in dotazione, tutti i soggetti ispezionati avevano ottemperato alle prescrizioni di misure "necessarie" contenute nel menzionato provvedimento generale e manifestato l'intenzione di dare attuazione anche alle misure "opportune" ivi prescritte. Complessivamente il provvedimento ha dimostrato efficacia e tenuta e l'Autorità non ha ritenuto allo stato di dare ulteriori indicazioni, ferma restando la costante attenzione rispetto alle segnalazioni in materia che dovessero pervenire.

Proprio l'adozione, da parte di un importante istituto di credito, delle misure sul tracciamento delle operazioni bancarie previste dall'anzidetto provvedimento ha consentito ad un cittadino che si è rivolto all'Autorità di ottenere un provvedimento con il quale è stata dichiarata l'illiceità del trattamento dei propri dati personali posto in essere dalla banca per il tramite di un proprio incaricato: quest'ultimo, infatti, aveva consegnato copia di un estratto conto, riferito al cliente, al coniuge dello stesso, il quale lo aveva successivamente prodotto in un giudizio di separazione, formulando, sulla base delle risultanze contabili dell'estratto conto, richieste economiche più onerose per il mantenimento dei figli. Nel caso esaminato, il *report* relativo al tracciamento degli accessi ai sistemi informativi prodotto dalla banca ha, infatti, evidenziato che il dipendente aveva effettuato un accesso alla scheda anagrafica del cliente e alla sua posizione contabile in un giorno e in un orario in cui il cliente medesimo si trovava in servizio presso la propria sede di lavoro posta in una località così lontana rispetto alla filiale da dover escludere che lo stesso potesse esservisi recato personalmente (provv. 10 novembre 2016, n. 463, doc. web n. 5852392).

Con tale provvedimento l'Autorità ha, peraltro, ricordato agli istituti di credito titolari del trattamento di assumere ogni iniziativa idonea ad evitare, per quanto possibile, "incidenti" simili a quello verificatosi nel caso illustrato (ad es., tramite efficaci controlli interni sulla liceità e legittimità degli accessi ai dati effettuati dagli incaricati del trattamento, nonché mediante l'identificazione della clientela nell'esecuzione delle operazioni bancarie) anche per assicurare, nella prospettiva della ormai prossima entrata in vigore del regolamento (UE) sulla protezione dei dati, il rispetto del principio di "responsabilità del titolare del trattamento" (*accountability*) previsto dall'art. 24 del regolamento medesimo.

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

Si ritiene utile altresì dare conto delle iniziative e del ruolo del Garante in un ambìto tra i più delicati, caratterizzato, stante la necessità di contemperare gli interessi contrapposti, dall'utilizzo di strumenti, quali i codici di deontologia, che producono una normazione "condivisa", elaborata con la partecipazione delle categorie a vario titolo interessate.

a) Codice di deontologia e di buona condotta per il trattamento dei dati personali a fini di informazione commerciale.

Il 1° ottobre 2016 è entrato in vigore il codice di deontologia e di buona condotta in materia di informazioni commerciali (provv. 17 settembre 2015, n. 479, doc. web n. 4298343), entrato a pieno titolo nel *corpus* normativo della protezione dei dati (costituisce l'All. n. 7 del Codice). I lavori di redazione, come ricordato nella Relazione dello scorso anno (cfr. Relazione 2015, p. 121), sono durati a lungo anche in ragione della difficoltà di disciplinare un ambito rimasto per decenni privo di norme di riferimento, ma interessato negli ultimi anni dal forte impatto delle innovazioni tecnologiche che hanno, in maniera significativa, modificato l'assetto di questo mercato ed i prodotti richiesti agli operatori del settore, moltiplicando in termini quantitativi e qualitativi i trattamenti, automatizzati e non, di dati personali.

I primi mesi di applicazione hanno mostrato l'utilità e l'efficacia delle nuove disposizioni e hanno fatto emergere un ambito di attività rimasto a lungo confinato a pochi addetti ai lavori. Da questo punto di vista, un ruolo prezioso viene svolto dal portale telematico realizzato in conformità alle previsioni di cui agli artt. 4 e 9 di tale codice di deontologia e posto in essere da Ancic, l'associazione di categoria che raggruppa i più importanti operatori economici del settore.

b) Lavori di aggiornamento e revisione del codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti (All. n. 5 al Codice).

Il codice dei Sistemi informativi creditizi "cd. codice dei Sic" è il codice di deontologia di più diffusa e larga applicazione e rappresenta lo strumento – nell'ambito della categoria di appartenenza – che più ha inciso nel settore del credito al consumo e più in generale dei finanziamenti alla cd. clientela *retail*. Il lavoro di aggiornamento e revisione di questo testo si sta però rilevando più lungo e complesso del previsto. Non si può negare che il perimetro oggettivo e soggettivo delle disposizioni è in rapida evoluzione e non sempre è facile trovare un terreno di intesa fra i vari attori presenti al tavolo di lavoro. La difficoltà risulta accresciuta dal mutato quadro normativo di riferimento che ha previsto per ulteriori categorie di titolari (in particolare, gli operatori telefonici e le società di assicurazioni) la possibilità di accedere alle banche dati dei Sic.

Proprio sul ruolo dei cd. nuovi "accedenti" nel 2016 si è discusso, specie in relazione all'istanza avanzata da alcuni dei partecipanti al tavolo di lavoro, se richiedere

a tali nuovi soggetti, non solo di esercitare il previsto accesso, ma anche di provvedere alla "contribuzione" al sistema di dati attinenti ai rapporti dagli stessi gestiti. Sul punto, il Garante ha avuto modo di esprimere un preliminare orientamento negativo, avendo di mira precipuamente la necessità di conservare il carattere omogeneo di queste banche dati senza assecondare un orientamento che porterebbe a snaturarle ed a trasformarle in *black list* generaliste, potenzialmente causa dell'esclusione sociale completa di soggetti in esse censiti con valutazione negativa.

c) Costituzione di una banca dati relativa a morosità intenzionali della clientela del settore telefonico (S.I.Mo.I.TEL)

Si tratta di una banca dati (concepita per censire un limitato numero di soggetti autori di comportamenti scorretti) che è stata legittimata dal provvedimento n. 523 dell'8 ottobre 2015 (doc. web. n. 4349760), che ha fissato i limiti della stessa e precisato i requisiti per l'inserimento in tale lista di cd. morosi intenzionali.

Il cammino verso la concreta realizzazione di questa banca dati (affidata all'accordo fra i vari operatori di Tlc interessati), sta procedendo, peraltro, in modo rallentato. Ad oggi, è stato solo individuato l'operatore tecnico incaricato di realizzare e gestire il sistema.

15.3. *La videosorveglianza in ambito privato*

Numerose sono state le segnalazioni ed i reclami pervenuti in materia di videosorveglianza, sia con riguardo alle tematiche più consuete, relative all'installazione di impianti in violazione dei princìpi sanciti dal d.lgs. n. 196/2003 ed in particolare del provvedimento di carattere generale sulla videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680), sia in relazione all'impiego delle telecamere connesso a nuove esigenze o a nuove possibilità determinate dal costante sviluppo tecnologico del settore.

È, inoltre, proseguito l'afflusso di istanze di verifica preliminare, in taluni casi, volte ad ottenere la conservazione delle immagini raccolte attraverso sistemi di videosorveglianza oltre il termine massimo di sette giorni individuato in termini generali, in applicazione del principio di proporzionalità del trattamento, dal citato provvedimento in materia di videosorveglianza (di regola al fine di rafforzare il livello di sicurezza di siti di particolare delicatezza), in altri casi, aventi ad oggetto l'istallazione di cd. sistemi intelligenti di videosorveglianza nonché l'utilizzo di telecamere per finalità diverse da quelle più strettamente legate alla sicurezza, tra cui il perseguimento di finalità di *marketing* e antifrode.

A quest'ultimo riguardo, per la prima volta è stata autorizzata l'istallazione di impianti per la rilevazione di persone a fini di *marketing* da parte di un istituto bancario (provv. 21 gennaio 2016, n. 13, doc. web n. 4806740).

Di seguito si dà conto di alcuni provvedimenti significativi emanati dall'Autorità, all'esito di procedure di verifica preliminare ai sensi dell'art. 17 del Codice, che possono costituire un valido punto di riferimento per operatori economici che intendessero istallare impianti di ripresa conformi alle caratteristiche risultanti dai provvedimenti medesimi.

Con provvedimento del 7 aprile 2016, n. 159 (doc. *web* n. 5063704), l'Autorità ha anzitutto accolto la richiesta presentata da alcune società che "svolgono attività di raccolta di gioco a mezzo di apparecchiature videoterminali (vlt) e di raccolta di denaro per conto dello Stato e/o del concessionario della rete telematica dell'Amministrazione dei Monopoli di Stato", al fine di conservare sino a 15 giorni le immagini registrate dai sistemi di videosorveglianza installati presso 17 sale da

gioco gestite dalle stesse e ubicate in diverse regioni italiane. Tale decisione trova giustificazione nell'esigenza di tutela del patrimonio aziendale vista la necessità delle società di rispettare dei tempi tecnici minimi (stimati in non meno di 10/15 giorni) per eseguire più efficaci controlli sul denaro e sulle apparecchiature presenti in sala nonché per visionare le immagini registrate dalle varie telecamere (al fine di prevenire la commissione di illeciti, specie con riferimento agli ammanchi di denaro). Ciò, tenendo conto dei tempi e delle modalità di lavoro degli addetti al servizio portavalori e di quelli operanti presso le "sale conta".

Con provvedimento 6 luglio 2016, n. 292 (doc. web n. 5411269), l'Autorità ha poi autorizzato una società che svolge un'attività di vendita, stoccaggio e movimentazione di prodotti petroliferi all'utilizzo di un sistema di videosorveglianza cd. intelligente basato su *motion detection* associato ad un meccanismo di rilevazione targhe, ritenendolo conforme ai princìpi posti dagli artt. 3 e 11 del Codice in ragione della particolare vulnerabilità del sito videosorvegliato, sia rispetto al possibile rischio di azioni terroristiche sia in relazione ai possibili rischi per l'incolumità della popolazione circostante e per l'ambiente in caso di incidente.

Il Garante ha anche accolto la richiesta di estensione, fino a 30 giorni, dei tempi di conservazione delle immagini presentata da una società che sviluppa progetti e realizzazioni ad alta tecnologia per le Forze armate e che, in ragione di tali produzioni, ha ricevuto il Nulla osta di sicurezza industriale (NOSI), secondo quanto previsto dal d.P.C.M. 6 novembre 2015, n. 5 recante disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate ed a diffusione esclusiva.

L'Autorità, considerati gli elevati *standard* di sicurezza che devono essere garantiti dalla società e che sono previsti dalle procedure per il rilascio del NOSI ha, pertanto, autorizzato la richiesta di allungamento dei tempi di conservazione delle immagini formulata dalla società (provv. 17 marzo 2016, n. 128, doc. web n. 4933452).

Infine, con un altro provvedimento (provv. 10 novembre 2016, n. 462, doc. web n. 5856462), il Garante ha accolto la richiesta di verifica preliminare presentata da una società specializzata nella creazione, produzione e distribuzione di tessuti e accessori per il settore dell'alta moda, per l'abilitazione di un sistema di videosorveglianza cd. intelligente costituito da telecamere dotate di funzionalità di elaborazione in automatico delle immagini acquisite, di rilevazione di determinati movimenti potenzialmente sospetti e di attivazione di allarmi nel caso sia rilevato l'abbandono di oggetti sospetti.

15.4. *Il recupero crediti*

Anche nel 2016 il trattamento di dati personali finalizzato al recupero stragiudiziale dei crediti è stato oggetto di numerose segnalazioni e reclami che rivelano l'opportunità di un nuovo intervento del Garante in questo settore.

Le doglianze pervenute hanno evidenziato (nonostante non sia obiettivamente facile fornire prove inequivocabili degli illeciti subiti) la persistenza di modalità di recupero particolarmente invasive e lesive della dignità dei debitori.

In un caso, dove l'istruttoria ha permesso di acquisire l'evidenza di trattamenti di questo tipo, l'attività di recupero crediti oggetto di un reclamo è risultata in contrasto con i princìpi generali del Codice e, in particolare, con quanto stabilito dal Garante nel provvedimento generale 30 novembre 2005 (Liceità, correttezza e pertinenza nell'attività di recupero crediti, doc. web n. 1213644). Ciò, con specifico riferimento alle svariate telefonate effettuate da talune società di recupero crediti sui numeri interni

dell'ospedale (ivi comprese utenze dedicate a servizi di emergenza), luogo di lavoro dell'interessato (provv. 22 giugno 2016, n. 274, doc. web n. 5407820).

Ad avviso dell'Autorità, tali comunicazioni, indipendentemente dal contenuto e dai toni utilizzati, hanno ingenerato negli interlocutori l'idea che il reclamante si trovasse in una situazione debitoria, determinando, in tal modo, una grave lesione della sua dignità personale e, conseguentemente, un trattamento illecito, oltre che generare disfunzioni organizzative in una delicata struttura lavorativa.

15.5. *Attività imprenditoriali e nuove tecnologie*

Sempre più spesso le possibilità offerte dalle nuove tecnologie ed in particolare le potenzialità di raccolta e aggregazione dei dati ricavati dalla rete internet portano all'elaborazione di progetti imprenditoriali, sottoposti al preventivo esame dell'Autorità, che evidenziano la pericolosità di molte applicazioni o, quantomeno, la necessità di fissare regole e di prevedere adeguate misure di sicurezza.

In particolare, nel 2016, il Garante ha avuto modo di pronunciarsi in ordine ai trattamenti di dati personali connessi all'istituzione di alcune piattaforme web con finalità di profilazione.

Con un primo provvedimento, il Garante ha vietato ad una società operante nel settore della ricerca e selezione di personale di trattare, per finalità di profilazione professionale, i dati personali degli utenti liberamente accessibili su alcuni siti internet e *social network*. Attraverso un sofisticato meccanismo di raccolta, elaborazione e aggregazione automatizzata delle informazioni ivi presenti (unicamente riconducibili, secondo quanto sostenuto, all'attività lavorativa degli interessati e da questi volontariamente pubblicate per promuovere la propria immagine professionale), la società si prefiggeva l'obiettivo di creare profili personalizzati eventualmente consultabili, attraverso un'apposita piattaforma web, nell'ambito delle attività di reclutamento del personale. Prima della loro pubblicazione sulla piattaforma, peraltro, gli interessati sarebbero stati resi edotti del trattamento connesso al servizio offerto, con possibilità per gli stessi di esercitare tutti i diritti previsti dall'art. 7 del Codice (provvedimento non pubblicato ai sensi dell'art. 24 del Regolamento Garante 1° agosto 2013).

Il sistema – che nella prospettiva indicata avrebbe apportato vantaggi sia ai selezionatori (agevolati nelle ricerche di personale) che ai candidati/lavoratori (attraverso l'aumento delle loro possibilità di impiego e/o progressione di carriera) – non avrebbe, secondo la società, arrecato lesioni alla sfera di riservatezza degli interessati, essendo basato su meccanismi di raccolta passiva di dati liberamente disponibili in rete e dichiaratamente pubblicati allo scopo dai medesimi interessati.

L'Autorità, contrariamente a quanto sostenuto dalla società, ha ritenuto che il trattamento connesso al servizio proposto, fondato sull'acquisizione massiva di dati personali presenti su molteplici siti internet e *social network* (peraltro non direttamente o necessariamente correlati alla sfera lavorativa degli interessati) non fosse conforme alla disciplina del Codice (artt. 11, 13, 23 e 24, d.lgs. n. 196/2003). Muovendo anche da un autorevole orientamento giurisprudenziale e da alcuni divieti stabiliti dalla legge (art. 8, l. n. 300/1970, richiamato dall'art. 113 del Codice; art. 10, d.lgs. n. 276/2003), l'Autorità ha ritenuto che non sussistessero i presupposti per poter trattare lecitamente tali dati, anche in ragione dei rischi gravanti sull'ampio bacino di utenti considerato e della non comprovata pertinenza e non eccedenza delle informazioni acquisite. L'Autorità, inoltre, ha ribadito che la conoscibilità di fatto e/o la materiale disponibilità di dati personali tratti da fonti (anche web) liberamente accessibili non comporta – di per sé – una altrettanto

15

libera riutilizzabilità dei dati medesimi, dovendosi a tal fine rapportare con gli scopi per i quali gli stessi sono stati pubblicati (in proposito, si è ritenuto che la divulgazione in internet, peraltro su spazi e piattaforme virtuali solo indirettamente od occasionalmente attinenti con l'attività lavorativa, di dati non agevolmente riconducibili all'ambito strettamente professionale non fosse compatibile con il principio di finalità). Perplessità, infine, sono emerse in ordine alle capacità del sistema di informare adeguatamente gli interessati e di elaborare profili professionali realmente esatti e aggiornati (provvedimento non pubblicato ai sensi dell'art. 24 del Regolamento Garante 1° agosto 2013).

Con altro provvedimento del 24 novembre 2016, n. 488 (doc. web n. 5796783), il Garante ha dichiarato non conforme alla disciplina del Codice il trattamento di dati connesso a un servizio web preordinato all'elaborazione di profili reputazionali. Mediante un sistema ritenuto in grado di calcolare, in termini imparziali e oggettivamente misurabili, il livello reputazionale dei soggetti censiti, un'associazione si proponeva, tra l'altro, di contrastare eventuali fenomeni di ingegneria reputazionale e mistificazione identitaria, rendendo più trasparenti, sicuri e affidabili i rapporti socio-economici.

L'infrastruttura descritta, costituita da una piattaforma web con annesso archivio informatico, avrebbe dovuto raccogliere ed elaborare una rilevante mole di dati personali contenuti in numerosi documenti (certificati, abilitazioni, diplomi, denunce, provvedimenti giudiziari, querele, encomi, premi, referenze) "caricati" volontariamente dagli utenti. Attraverso un apposito algoritmo, il sistema avrebbe poi assegnato agli interessati, previa verifica formale dei documenti allegati, un punteggio complessivo (suddiviso in cinque *sub-rating*: "penale", "fiscale", "civile", "lavoro e impegno civile" "studi e formazione") rappresentativo della loro affidabilità reputazionale. Tale punteggio, unitamente ai relativi documenti "giustificativi", sarebbe stato quindi reso accessibile agli altri utenti della piattaforma, con possibilità per questi ultimi di disporne a vario titolo (ad es., per effettuare indagini su clienti e fornitori o nelle operazioni di ricerca e selezione di personale).

Nel vietare il trattamento, il Garante ha ritenuto che l'utilizzo del sistema comportasse rilevanti problematiche per la *privacy* degli interessati a causa, tra l'altro, della delicatezza delle informazioni che si sarebbero volute acquisire, del pervasivo impatto sugli interessati, nonché dei presupposti e delle modalità di trattamento prospettate. Nel rilevare l'assenza di un'idonea cornice normativa (art. 11, comma 1, lett. *a*), del Codice) e nel sottolineare la possibilità stessa per il servizio di condizionare profondamente la vita delle persone, incidendo, anche, sulla loro dignità (art. 2 del Codice), l'Autorità ha poi espresso dubbi, più in generale, sull'opportunità di rimettere a un meccanismo automatizzato decisioni su aspetti particolarmente delicati e complessi quali quelli connessi alla reputazione individuale. Criticità, inoltre, sono state ravvisate con riferimento al consenso degli interessati (reputato non conforme, in taluni casi, agli artt. 23 e 26 del Codice), al trattamento dei dati sensibili e giudiziari (artt. 26 e 27 del Codice; autorizzazioni generali nn. 3 e 7), alle misure di sicurezza dichiarate (artt. 31 e ss. del Codice; All. B al Codice medesimo), ai tempi di conservazione e all'informativa da rendere ai soggetti censiti (artt. 11, comma 1, lett. *e*) e 13 del Codice). Perplessità, infine, sono state manifestate con riferimento al rispetto dei princìpi di necessità, proporzionalità e qualità dei dati (artt. 3 e 11, comma 1, lett. *c*) e *d*), del Codice), attese le prospettate modalità di raccolta massiva di dati e documenti, la loro non comprovata pertinenza e non eccedenza in rapporto alle finalità perseguite e il concreto rischio di possibili profili reputazionali inesatti o non aggiornati, eventualmente basati su documentazione falsa o alterata.

In relazione ad un diverso contesto, con provvedimento 9 giugno 2016, n. 256 (doc. web n. 5252271), il Garante si è, invece, positivamente espresso in riferimento a un trattamento di dati personali e biometrici basato sull'analisi comportamentale dei clienti di una banca (operante solo *online*) in occasione della loro navigazione nell'area privata del sito web. Il servizio, caratterizzato dalla registrazione delle attività degli utenti e dalla loro interazione con i dispositivi utilizzati, mirava a offrire più elevati livelli di tutela nell'utilizzo dell'internet *banking*, attraverso la creazione di profili comportamentali individuali che, confrontati di volta in volta con quelli generati in occasione delle singole sessioni di navigazione nell'area privata del sito della banca, avrebbero permesso l'attivazione di adeguate contromisure in presenza di eventuali accessi indebiti (messaggi di avviso all'interessato, inibizione delle operazioni dispositive, ecc.).

Pur rimarcando la legittimità del trattamento dei dati biometrici solo in casi particolari, tenuto conto delle finalità perseguite e del contesto di riferimento, l'Autorità ha valutato positivamente l'utilizzo di detti dati nell'ambito considerato, ritenendolo conforme ai princìpi del Codice (artt. 3 e 11, comma 1, lett. *a*), *b*), e *d*). L'Autorità ha tuttavia raccomandato al titolare di configurare *ab origine* il sistema in maniera tale da acquisire il minor numero di informazioni utile allo scopo, ricordando altresì che i dati acquisiti non potranno essere in alcun modo utilizzati per finalità diverse da quelle dichiarate, o comunque in operazioni di trattamento non compatibili con gli scopi originari della raccolta.

Non meno delicate sono le iniziative volte a costituire banche dati settoriali, tipicamente finalizzate a verificare l'affidabilità dei contraenti o a svolgere una funzione antifrode. Al riguardo, con provvedimento 1° giugno 2016, n. 234 (doc. web n. 5306512), il Garante ha rigettato la richiesta di verifica preliminare e di bilanciamento di interessi presentata da un'associazione rappresentativa di imprese operanti nel settore dell'autonoleggio finalizzata alla costituzione di una banca di dati centralizzata volta a prevenire e contrastare furti, appropriazioni indebite e frodi inerenti ai veicoli noleggiati. Tale banca di dati – alimentata con le informazioni relative agli intestatari dei contratti di autonoleggio e ai conducenti dei veicoli oggetto di comportamenti illeciti –, sarebbe servita, nelle intenzioni, ad ostacolare (o, quantomeno, arginare) la diffusione del fenomeno, attraverso la condivisione di un patrimonio informativo correlato anche alla ricorrenza di più eventi o alle risultanze degli accertamenti svolti. Nel ritenere insoddisfacenti gli elementi addotti dall'associazione a sostegno del richiesto bilanciamento (art. 24, comma 1, lett. *g*), del Codice), il Garante ha escluso che, nel caso di specie, potessero rilevare dati inizialmente qualificabili come giudiziari; sono stati sottolineati, inoltre, i rischi gravanti in capo ai soggetti censiti dalla costituzione dell'archivio e le criticità derivanti, da un lato, dalla centralizzazione delle informazioni (potenzialmente anche molto delicate) e, dall'altro, dai tempi di conservazione dei dati (in ipotesi molto prolungati).

Il Garante ha, infine, vietato anche il progetto volto a realizzare un sistema biometrico basato sul riconoscimento facciale di chi richiede un finanziamento al fine di prevenire possibili furti di identità (provv. 25 febbraio 2016, n. 77 non pubblicato ai sensi dell'art. 24 del Regolamento Garante 1° agosto 2013). Il sistema – che una società aveva ipotizzato di implementare e in relazione al quale aveva presentato al Garante una richiesta di verifica preliminare per appurarne la conformità alla normativa in materia di protezione dei dati personali – prevedeva di scansionare la fotografia presente sul documento d'identità dei potenziali interessati, nel momento in cui avessero richiesto un finanziamento presso istituti di credito o altri intermediari finanziari convenzionati con la società. I dati biometrici del volto così acquisiti, sarebbero stati raccolti, criptati, codificati, associati con altre informazioni personali

15

riferite al singolo soggetto e infine confrontati sia con fotografie già censite in altri archivi (ad es., le foto segnaletiche utilizzate per il riconoscimento di soggetti ricercati dalle Forze di polizia), sia con immagini pubblicate sulla stampa o reperibili su internet. Il Garante ha anzitutto evidenziato che, per verificare l'identità di soggetti che richiedono finanziamenti, gli istituti bancari e le società finanziarie dispongono del sistema pubblico di prevenzione delle frodi nel settore del credito al consumo e dei pagamenti dilazionati o differiti (cd. SCIPAFI), con specifico riferimento al furto di identità, recentemente istituito dal legislatore (d.lgs. 11 aprile 2011, n. 64, che ha integrato il d.lgs. 13 agosto 2010, n.141 mediante l'introduzione del Titolo V-*bis*, in attuazione della direttiva europea n.2004/48/CE relativa ai contratti di credito ai consumatori). A tale sistema è prevista, in base a specifiche disposizioni attuative contenute nel decreto del Ministro dell'economia e delle finanze del 19 maggio 2014, n. 95, la partecipazione di numerosi soggetti (quali aderenti diretti o indiretti in virtù di specifiche convenzioni stipulate con il competente Ministero), "esclusivamente in relazione ai dati personali, pertinenti e non eccedenti, necessari al perseguimento delle specifiche finalità inerenti al settore commerciale di appartenenza" (art. 3). Considerando che la società aveva dichiarato di non avere stipulato la convenzione per aderire al predetto sistema di cui, in generale, non è stata dimostrata l'inadeguatezza a contrastare il fenomeno dei furti d'identità nel settore del credito, l'Autorità ha stabilito che non potesse ritenersi necessario e proporzionato un uso generalizzato e incontrollato dei dati biometrici dei clienti. Il Garante, inoltre, ha rinvenuto molteplici criticità relative al sistema prospettato: in particolare, è risultato inaffidabile il processo di confronto delle fotografie delineato, con un elevato rischio di falsi sia positivi che negativi, e sono state ritenute inadeguate le misure di sicurezza previste a protezione dei dati – tra le altre, quelle a protezione della rete di comunicazione elettronica sulla quale i dati biometrici sarebbero stati trasmessi al sistema centralizzato di acquisizione dati – con conseguenti ripercussioni per i diritti individuali in caso di accessi di persone non autorizzate o, comunque, di abusi sulle informazioni memorizzate. Le stesse modalità di acquisizione del consenso al trattamento dei dati biometrici sono risultate non conformi al Codice, essendo stato configurato il consenso come obbligatorio e senza che fossero state previste modalità alternative di verifica dell'identità per accedere al finanziamento.

16 I dati biometrici

16.1. *Biometria in ambito pubblico*

Non sono stati molto numerosi gli interventi del Garante nel 2016 con riferimento al trattamento di dati biometrici in ambito pubblico. Tra questi il più significativo ha riguardato un istituto scolastico che chiedeva l'autorizzazione per la rilevazione, tramite impronte digitali, degli alunni all'ingresso della scuola finalizzata alla registrazione dei ritardi e all'immediato invio di sms ai genitori.

In questo caso, richiamando il provvedimento generale, è stato evidenziato che "i dati biometrici sono, per loro natura, direttamente, univocamente e in modo tendenzialmente stabile nel tempo, collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona, richiedendo particolari cautele in caso di loro trattamento. L'adozione di sistemi biometrici, in ragione della tecnica prescelta, del contesto di utilizzazione, del numero e della tipologia di potenziali interessati, delle modalità e delle finalità del trattamento, può comportare quindi rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato" (cfr. punto n. 4, provv. 12 novembre 2014, n. 513, doc. web n. 3556992). Nel caso di specie il titolare del trattamento è stato invitato ad accertare, con particolare rigore, che il trattamento dei dati biometrici degli alunni fosse effettivamente necessario e proporzionato rispetto alle finalità concretamente perseguite, tenendo in considerazione la minore età degli interessati e la peculiarità del contesto (artt. 2, 3 11 e 18, del Codice) e solo all'esito di questa valutazione, presentare all'Autorità una richiesta di verifica preliminare, ai sensi dell'art. 17, del Codice (nota 28 luglio 2016).

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

La delicatezza dei dati biometrici e la conseguente necessità di assicurare particolari garanzie per il loro trattamento a tutela degli interessati – già significativamente messe in luce dal Garante con le linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro, rispettivamente, alle dipendenze di datori di lavoro privati e in ambito pubblico (provv.ti 23 novembre 2006, n. 53, doc. web n. 1364099 e 14 giugno 2007, n. 23, doc. web n. 1417809) – sono state ulteriormente rimarcate con il provvedimento generale prescrittivo in tema di biometria (12 novembre 2014, n. 513, doc. web n. 3556992). Con tale provvedimento l'Autorità ha ribadito che il trattamento di dati personali biometrici, in considerazione della loro stretta (e stabile) relazione con l'individuo e la sua identità, può essere effettuato solo previa adozione di particolari cautele. In particolare tutti coloro che intendano effettuare tale tipologia di trattamenti sono tenuti a presentare un'istanza di verifica preliminare al Garante, tranne che in alcuni casi di esonero puntualmente individuati, sempre che vengano adottate specifiche misure e accorgimenti tecnici e che siano rispettati i princìpi generali di liceità, finalità, necessità e proporzionalità dei trattamenti.

La specificità della tutela e delle garanzie approntate a favore degli interessati in caso di trattamento di tale particolare tipologia di dati personali ha trovato riscon-

tro nel regolamento (UE) 2016/679 che, diversamente dal passato, ha inserito i dati biometrici nella categoria dei dati sensibili (v. art. 9, comma 1, reg. UE).

Finalità di rilevazione delle presenze

Con riferimento all'uso di tecnologie biometriche per finalità di rilevazione delle presenze, il Garante ha chiarito sin dal 2007 che l'accertamento del rispetto dell'orario di lavoro anche mediante "controlli di tipo automatizzato" deve, in ogni caso, essere effettuato nel rispetto della disciplina in materia di protezione dei dati personali, anzitutto con riguardo all'osservanza dei princìpi di necessità e proporzionalità (cfr. punto 7.1., linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, cit.; v. anche Gruppo dei garanti europei previsto dall'art. 29 della direttiva 95/46/Ce WP193, parere 3/2012 sugli sviluppi nelle tecnologie biometriche, adottato il 27 aprile 2012).

Tali princìpi impongono che siano preventivamente considerati altri sistemi, dispositivi e misure di sicurezza fisiche e logicistiche – meno invasive della libertà e la dignità stessa dei lavoratori interessati (ad es., il badge, normalmente utilizzato presso le pp.aa., se del caso associabile a pin individuale) – che possano assicurare parimenti una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro senza fare ricorso al trattamento dei dati biometrici (artt. 2, 3 e 11, del Codice).

Sebbene, quindi, in applicazione di tali princìpi, con riguardo ad alcuni casi di uso generalizzato dei sistemi biometrici e in presenza di astratte esigenze di controllo su presunti abusi, il Garante abbia ritenuto sproporzionato il relativo trattamento (cfr., provv.ti 22 ottobre 2015, n. 522, doc. web n. 4430740; 31 gennaio 2013, n. 38, doc. web n. 2304669; provv.ti 30 maggio 2013 n. 261 doc. web n. 2502951, n. 262, doc. web n. 2503101 e 1° agosto 2013, n. 384, doc. web n. 2578547), diversamente in presenza di obiettive e documentate esigenze che impongano di adottare sistemi di rilevazione che garantiscano la certezza dell'identità del dipendente, l'Autorità ha ammesso il relativo trattamento, tenuto conto della specificità del caso concreto, del contesto socio-economico di riferimento e delle caratteristiche della tecnologia impiegata.

Nel 2016, in un primo caso, in relazione all'avvenuta installazione, da parte di un comune, di un sistema biometrico basato sul trattamento delle impronte digitali per finalità di rilevazione delle presenze in servizio dei dipendenti (adottato a seguito di asseriti abusi nell'attestazione della presenza in servizio presso comuni della regione di appartenenza), il Garante ha ritenuto illecito il trattamento e ne ha disposto conseguentemente il divieto poiché il titolare del trattamento non aveva ottemperato all'obbligo di effettuare la notificazione del trattamento (art. 37, del Codice) e di presentare la richiesta di verifica preliminare (art. 17, del Codice). La fattispecie in esame non è stata, infatti, ritenuta inquadrabile in una delle ipotesi di esenzione dalla presentazione di istanza di verifica preliminare individuate dal Garante nel citato provvedimento generale. L'assenza di tali elementi, che costituiscono requisiti di liceità del trattamento, sono stati ritenuti assorbenti ai fini della valutazione della complessiva liceità del trattamento effettuato (provv. 17 marzo 2016, n. 129, doc. web n. 4948405).

A fronte di una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice e all'esito di una complessiva valutazione alla luce dei princìpi di necessità e proporzionalità rispetto alle finalità perseguite, il Garante ha poi dichiarato la liceità dell'utilizzo di un sistema biometrico da parte di un'Azienda ospedaliero-universitaria per finalità di rilevazione delle presenze dei dipendenti, nell'ambito di un più ampio quadro di iniziative per il contrasto all'assenteismo, ritenendolo proporzionato in relazione alla specificità del caso concreto (artt. 3, 11, comma 1, lett. *a*) e *d*), 18 e 19, comma 1, del Codice).

La peculiarità del caso è stata messa in luce dai circostanziati elementi forniti dal titolare del trattamento riguardanti, in particolare, l'elevato numero di lavoratori coinvolti dagli accertamenti interni e dalle indagini dell'autorità giudiziaria, la risonanza mediatica del caso con conseguente discredito della struttura sanitaria nonché le specificità della concreta realtà lavorativa. Tra queste ultime sono state ritenute meritevoli di considerazione, anche, l'articolazione in più padiglioni della struttura ospedaliera, l'accesso promiscuo ad essi da parte di utenti e personale medico nonché la peculiarità delle mansioni svolte dai dipendenti che impongono continui spostamenti tra i reparti. Tali condizioni concrete e la particolare condotta che l'Azienda intendeva prevenire (l'utilizzo del badge da parte di terzi o di altri dipendenti per conto del lavoratore assente dal servizio) avrebbero reso inefficaci gli strumenti automatizzati alternativi, pure esperiti dall'Azienda, impregiudicati comunque gli strumenti posti dall'ordinamento a disposizione del personale dirigenziale o direttivo per la verifica della presenza del personale (cfr. artt. 55 e ss., d.lgs. n. 165/2001 e, in particolare, art. 54-*quater* nel testo introdotto dal d.lgs. 20 giugno 2016, n. 116; artt. 18 e 19, comma 1, del Codice; regolamento adottato con deliberazione del direttore generale dell'azienda n. 1030 del 27.11.2014) (provv. 15 settembre 2016 n. 357, doc. web n. 5505689).

Trattamenti a scopo di sperimentazione e ricerca scientifica

L'Autorità ha poi ritenuto lecito il trattamento di dati biometrici effettuato per finalità di ricerca scientifica da un consorzio di servizi informatici, limitatamente ad un breve periodo di sperimentazione (si noti che in ragione delle specificità del sistema utilizzato e della particolare tipologia di dati trattati il caso non rientrava fra quelli esonerati dalla verifica preliminare in base al citato provvedimento generale del Garante).

In qualità di partecipante ad un progetto europeo, il consorzio ha inteso chiedere ai propri dipendenti di utilizzare, come sistema di autenticazione, un servizio di riconoscimento biometrico (basato su riconoscimento facciale e autenticazione vocale), per accedere al servizio di visualizzazione della busta paga e altri documenti in alternativa al sistema in uso basato sull'utilizzo di credenziali di autenticazione.

Le finalità del trattamento erano state prospettate come di tipo scientifico, diverse quindi da quelle perseguite nell'ambito delle attività di gestione del rapporto di lavoro con i dipendenti. Il sistema progettato prevedeva che, in occasione di ciascun singolo accesso al servizio, l'interessato potesse scegliere tra i due modelli di autenticazione disponibili e in ogni momento chiedere la cancellazione dei modelli biometrici a sé riferiti.

Il Garante ha ritenuto lecito il trattamento, alla stregua delle disposizioni concernenti il trattamento di dati personali effettuato per scopi scientifici (artt. 97-100, 104 e 105, del Codice; codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici – provv. n. 2, 16 giugno 2004, All. 4 del Codice) pur prescrivendo alcune misure ed accorgimenti a tutela dei diritti degli interessati. Così, ad es., al consorzio l'Autorità ha richiesto di adottare misure volte a garantire che il trattamento oggetto di sperimentazione sia in concreto effettuato con modalità autonome dall'operatività dei sistemi utilizzati per finalità di gestione del rapporto di lavoro e che la cancellazione dei dati biometrici al termine della sperimentazione (o a seguito di specifica richiesta del partecipante) sia irreversibile (provv. 27 ottobre 2016, n. 438, doc. web n. 5763201).

17 Attività di normazione tecnica internazionale e nazionale

Nel 2016 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 del *Joint Technical Committee* (JTC1) dell'organizzazione internazionale per la normazione di ISO. Il gruppo di lavoro segue gli aspetti di sicurezza nella gestione delle identità, nella biometria e *privacy*.

L'Autorità, armonizzando la propria posizione con quelle delle altre autorità di protezione dati tramite il WP29, 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*: requisiti per fornire l'informativa e acquisire il consenso *online* in modalità *user friendly*;
- ISO 29134 - *Privacy Impact Assessment – Guidelines*: linee guida per condurre un *Privacy Impact Assessment* (PIA) allo scopo di valutare e mitigare i rischi relativi al trattamento di dati personali attraverso un approccio di gestione del rischio secondo i princìpi previsti dalla norma tecnica ISO 31000 (*Risk management - Principles and guidelines*), nonché per definire i controlli sulla base delle norme tecniche ISO/IEC 27002 (*Code of practice for information security controls*) e ISO 29151 (*Code of practice for the protection of personally identifiable information)*.
- ISO 29151 - *Code of practice for the protection of personally identifiable information*: catalogo di controlli per la protezione dei dati personali che specializzano i controlli di sicurezza previsti dalla ISO/IEC 27002 e ne prevedono ulteriori, in conformità ai princìpi della ISO/IEC 29100 (*Privacy Framework*).

L'Autorità, inoltre, ha 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 sulle 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), 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 mondo socio-sanitario della salute per una corretta identificazione e caratterizzazione delle *app* nonché maggiore consapevolezza degli utilizzatori.

18 Il trattamento dei dati personali nel condominio

In questa materia in cui la casistica è sempre piuttosto cospicua, di particolare interesse è risultato un caso che ha avuto origine dall'acquisto di un'unità immobiliare sita in un condominio e dall'avvenuto conferimento nello stesso contratto di compravendita, da parte dell'acquirente, di una specifica procura al venditore-costruttore ad apportare successive modifiche al regolamento condominiale. A seguito di un'intervenuta modifica dello stesso ad opera dell'impresa costruttrice, l'amministratore del condominio ha distribuito in sede assembleare a tutti i condomini una copia del nuovo regolamento condominiale che in allegato riportava, tra gli altri documenti, anche copia autentica dell'atto di acquisto sottoscritto a suo tempo dal segnalante (nonché quelli di altri condomini-acquirenti). L'avvenuta allegazione al nuovo regolamento dell'originario atto di acquisto dell'immobile in forma integrale ha costituito il motivo da cui ha avuto origine la segnalazione, stante le aspettative di riservatezza avanzate dal segnalante in ordine ai dati personali (quali ad es., il prezzo pattuito per la vendita e la relativa descrizione delle modalità, dei tempi e degli strumenti di pagamento, ecc.) contenuti nell'atto di compravendita e resi noti all'intera compagine condominiale.

Al riguardo, il Garante, anche in ragione delle peculiari questioni di natura civilistica sottese al caso in esame, ha ritenuto opportuno formulare alcune richieste di parere nei confronti dell'Associazione nazionale amministratori condominiali e immobiliari (Anaci) e del Consiglio nazionale del notariato (Cnn) e svolgere così i necessari approfondimenti in ordine al tema. All'esito di un'articolata istruttoria che si è svolta nel corso del 2016, l'Autorità ha constatato la novità del quesito, che ha infatti rappresentato un importante precedente per chiarire in termini generali quali possano essere gli atti, nonché la forma degli stessi (quindi anche quella non integrale), da allegare al regolamento condominiale e suscettibili di condivisione nel relativo contesto. Prendendo atto delle indicazioni fornite nei pareri resi dai soggetti sopra menzionati e considerata altresì l'accertata mancanza di un definito indirizzo giurisprudenziale e dottrinale in merito alla fattispecie, il Garante ha colto l'occasione per sensibilizzare i professionisti in questione (notai ed amministratori di condominio) a prestare particolare attenzione alle fasi della redazione e della raccolta della documentazione inerente il regolamento condominiale destinata a circolare all'interno della stessa compagine, invitandoli, per il tramite degli organi e delle associazioni che li rappresentano, a valutare l'opportunità di formulare una specifica richiesta di copia parziale o di estratto dell'atto di compravendita da allegare al (nuovo) regolamento nel caso in cui la procura ad apportare modifiche a quest'ultimo sia stata conferita al costruttore-venditore nell'originario atto di acquisto rogitato presso altro notaio e si riveli di per sé "strutturalmente autosufficiente" (cfr. artt. 51, n. 3, l. 16 febbraio 1913, n. 89 e 2714 e 2718 c.c.), o comunque ad adottare altre opportune cautele (valutando, con riguardo al ruolo degli amministratori, ad esempio, la possibilità di fornire alla compagine condominiale il regolamento nella forma del solo articolato, ossia privo della documentazione attestante le procure rese dai condomini), affinché gli adempimenti posti dalla legge in capo ai menzionati professionisti possano essere eseguiti, ove possibile, nella piena osservanza di quanto previsto dal principio generale di proporzionalità, pertinenza e non eccedenza di cui all'art. 11, comma 1, lett. *d*) del Codice.

19 Il trasferimento dei dati all'estero

In materia di trasferimenti transfrontalieri di dati personali, l'Autorità, considerato il crescente utilizzo, da parte dei gruppi multinazionali d'imprese, delle cd. *Binding corporate rules* (Bcr), quali strumenti per il trasferimento di dati personali verso Paesi terzi, e stante il cospicuo numero di autorizzazioni complessivamente rese dal Garante in materia, ha ritenuto opportuno avviare un'indagine di carattere conoscitivo (anche in chiave di confronto rispetto a quanto emerso all'esito dell'attività di monitoraggio sulle attività di trasferimento di dati all'estero effettuate da alcuni operatori italiani già condotta dal Garante nel 2002, cfr. Relazione 2003, p. 96); ciò al fine di acquisire informazioni di carattere generale in ordine allo stato dei flussi transfrontalieri intra-gruppo di dati personali in essere nell'ambito di alcuni tra i più importanti gruppi multinazionali di imprese italiani e agli strumenti utilizzati dagli stessi al fine di garantirne la legittimità.

L'indagine in questione ha consentito di definire un primo quadro di insieme in ordine ai flussi di dati effettuati verso Paesi *extra*-UE nell'ambito dei gruppi interessati evidenziando innanzitutto come le aree geografiche maggiormente interessate dai trasferimenti riguardino ancora una volta gli USA, l'Asia, l'America centro meridionale, ma anche in parte l'Europa dell'est e l'Africa. Con specifico riguardo alle caratteristiche dei flussi transfrontalieri di dati concretamente posti in essere, è stato possibile constatare che i dati personali oggetto di trasferimento si riferiscono, in primo luogo, al personale dipendente (categoria nella quale sono di frequente ricompresi anche gli *ex* dipendenti e i familiari), in misura minore ai dati dei clienti (anche di quelli potenziali), nonché, da ultimo, a quelli relativi a fornitori e a soggetti terzi quali, ad es., i consulenti. Le finalità maggiormente perseguite nell'ambito dei trasferimenti sono quelle concernenti la gestione del rapporto di lavoro (in particolare del personale distaccato), gli adempimenti societari, la tutela giurisdizionale e l'esecuzione del contratto. I flussi di dati sono effettuati in larga parte in virtù dell'acquisizione del consenso degli interessati o comunque sulla base del presupposto di legittimità indicato nell'art. 43, comma 1, lett. *b*) del Codice (esecuzione degli obblighi contrattuali).

Ciò premesso, dall'indagine effettuata è altresì emersa:

a) una certa tendenza da parte delle imprese italiane a prediligere soluzioni (anche di natura tecnica) che comportino trasferimenti di dati personali nel contesto europeo piuttosto che in quello *extra*-UE (tendenza che si era già potuta rilevare a seguito dell'esame dei contributi resi dalle principali associazioni di categoria operanti nel settore industriale e commerciale interpellate dal Garante all'indomani della pronuncia della CGUE 6 ottobre 2015, cfr. Relazione 2015, p. 132);
b) una limitata incidenza dell'utilizzo delle clausole contrattuali *standard* rispetto al volume complessivo dei trasferimenti effettuati; ciò in considerazione del fatto che si tratta di strumenti prevalentemente utilizzati dalle società oggetto dell'indagine, con riferimento a trasferimenti di dati verso soggetti esterni al gruppo d'impresa (si fa in particolare riferimento alle clausole *standard* relative alla decisione 5 febbraio 2010, n. 87/2010/UE);

c) l'introduzione, da parte di alcuni dei gruppi interessati, all'interno della loro organizzazione, di prassi aziendali volte a fornire, sotto forma di linee guida (o in taluni casi mediante l'adozione di veri e propri codici di condotta), *standard* aziendali in materia di protezione dei dati (tra l'altro di regola consultabili in una apposita sezione della intranet) comuni ai vari membri del gruppo, anche con specifico riguardo al tema del trasferimento dei dati all'estero.

Con riferimento, poi, alle richieste di autorizzazione ai trasferimenti di dati personali verso Paesi terzi pervenute nel 2016, l'attività del Garante si è focalizzata sulle numerose istanze, provenienti da gruppi multinazionali d'imprese, volte al rilascio di autorizzazioni nazionali in materia di Bcr. In merito, il Garante ha avviato le relative istruttorie che si sono concluse con l'approvazione di sette autorizzazioni. In sede di istruttoria è stata verificata la conformità del testo delle Bcr con l'ordinamento italiano e con alcuni dei principali criteri stabiliti in materia dal Gruppo Art. 29 (cfr. provv.ti 18 febbraio 2016, n. 65, doc. web n. 4797978; 12 maggio 2016, n. 217, doc. web n. 5141884; 9 giugno 2016, n. 258, doc. web n. 5242975; 13 luglio 2016, n. 307, doc. web n. 5411590; 6 ottobre 2016, n. 392, doc. web n. 5834650; 1° dicembre 2016, n. 504, doc. web n. 5860749).

Sotto altro profilo, l'attenzione del Garante è stata rivolta all'importante novità rappresentata dalla decisione di esecuzione (UE) 2016/1250 della Commissione europea del 12 luglio 2016 (in GUUE 1° agosto 2016, L 207), ai sensi della quale l'Accordo denominato "EU-U.S. *Privacy Shield*" (cd. Scudo UE-USA per la *privacy*, di seguito Scudo), costituito dai princìpi emanati dal Dipartimento del commercio degli Stati Uniti il 7 luglio 2016 garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea ad organizzazioni aventi sede negli Stati Uniti d'America. Lo Scudo, che impone alle imprese americane obblighi più stringenti di tutela dei dati personali provenienti dall'Europa, prevede, inoltre, in linea con quanto chiesto dalla CGUE che aveva invalidato il precedente accordo detto *Safe Harbor* (cd. regime di Approdo sicuro), puntuali obblighi per le autorità americane di vigilanza sul rispetto dell'accordo medesimo e di collaborazione con le Autorità europee per la protezione dei dati.

In tale scenario, l'Autorità è intervenuta, con riferimento all'ambito nazionale, con l'autorizzazione 27 ottobre 2016, n. 436 (doc. web n. 5652873), conformandosi, ai sensi dell'art. 44, comma 1, lett. *b*) del Codice, alla citata decisione e autorizzando, pertanto, i trasferimenti di dati personali oltreoceano dal territorio italiano verso organizzazioni stabilite negli Stati Uniti che si autocertificano nel sistema; tutto ciò in base al nuovo accordo siglato tra UE e USA, tenuto conto anche della valutazione resa in merito dal Gruppo Art. 29 con il parere n. 1/2006 (WP 238) adottato il 13 aprile 2016. L'autorizzazione del Garante si affianca a quella del 22 ottobre 2015 (doc. web n. 4396484) che – in ragione della intervenuta sentenza della CGUE – regolava i trasferimenti nazionali dei dati verso gli Stati Uniti posti in essere negli anni sulla base dell'accordo *Safe Harbor* e disponeva al contempo la caducazione della precedente autorizzazione resa dal Garante il 10 ottobre 2001 (doc. web n. 30939) (cfr. Relazione 2015, p. 132).

L'Autorità italiana si è comunque riservata di effettuare in qualsiasi momento controlli per verificare la liceità e la correttezza del trasferimento dei dati effettuati dal territorio nazionale sulla base dello Scudo e di ogni operazione ad essi inerente, nonché di adottare, se necessario, i provvedimenti previsti dal Codice anche alla luce delle verifiche condotte dalla stessa Commissione europea che, da parte

19

sua, sottoporrà a monitoraggio continuo il funzionamento dello Scudo per verificare se gli Stati Uniti continuino a garantire un livello di protezione adeguato ai dati personali trasferiti dall'Unione europea. Tali controlli avranno cadenza annuale, ma è prevista anche una specifica verifica a seguito dell'entrata in vigore del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio adottato il 27 aprile 2016.

20 Il registro dei trattamenti

20.1. *La notificazione*

La notificazione è una dichiarazione con la quale un titolare del trattamento (pubblico o 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 (https://web.garanteprivacy.it/rgt/NotificaTelematica.php).

Le notificazioni sono inserite in un registro pubblico liberamente e gratuitamente consultabile *online*, sul 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 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 nonché 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*.

20.2. *L'evoluzione della notificazione nel 2016*

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.

20

Al fine di ottimizzare il riscontro alle numerose richieste di chiarimenti che quotidianamente pervengono al Garante tramite telefono o posta elettronica, in merito alle necessità e modalità di notificazione, nonché allo scopo di agevolare il corretto e tempestivo adempimento di tale obbligo da parte dei titolari del trattamento, in una apposita sezione del sito web istituzionale è stato pubblicato un gruppo di risposte alle domande più frequenti (cd. FAQ).

La pubblicazione di tali FAQ è stata realizzata al fine di agevolare l'interfaccia verso l'utenza su aspetti, sia di natura tecnica che di merito, legati alla procedura di notificazione, per i quali è pervenuta nel tempo la maggior parte dei quesiti. Nel 2016 sono pervenute circa 800 richieste di chiarimento telefoniche e circa 250 tramite posta elettronica, con una netta diminuzione, quindi, rispetto agli anni precedenti in cui tale sezione non era ancora disponibile, offrendo così un servizio più celere e maggiormente fruibile per gli utenti.

È altresì 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 medesimo Registro; tale attività è stata effettuata anche mediante ispezioni *in loco*, nell'ambito della programmazione ispettiva di cui si è dato conto al par. 23.1.

In particolare, dai controlli effettuati nel corso dell'anno sono emersi 37 casi di omessa o incompleta notificazione del trattamento e sono state contestate le relative violazioni ai titolari del trattamento. La maggior parte delle violazioni è stata riscontrata con riferimento al trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (art. 37, comma 1, lett. *a*), del Codice), principalmente nell'ambito dell'offerta di servizi di *car sharing,* nel corso di un ciclo di ispezioni condotto nei confronti di alcune società operanti nel settore, selezionate sull'intero territorio nazionale.

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

Anche in ragione delle sopra esposte attività ispettive, delle numerose violazioni riscontrate e contestate ai titolari e del conseguente adempimento da parte degli stessi e degli altri operatori del settore, si evidenzia, infine, che nel 2016 il Registro dei trattamenti è stato implementato con 2.369 notificazioni, a fronte di una media inferiore a 1.600 notificazioni annue nell'ultimo quinquennio.

21 La trattazione dei ricorsi

21.1. *I profili generali*

Anche per il 2016 un primo sguardo di insieme ai dati statistici ed un loro rapido confronto con quelli dell'anno precedente possono fornire alcune interessanti indicazioni sul *trend* generale di quello che continua ad essere uno degli strumenti caratteristici di tutela in materia di protezione dei dati personali.

Il primo elemento che viene in evidenza è la sostanziale conferma del consolidamento che si registra in determinati settori oggetto di ricorsi, i quali, dopo periodi di notevole impatto, anche numerico, pian piano che se ne delineano i confini, si riducono sino a diventare del tutto marginali. È il caso, ad es., dei ricorsi relativi ai Sistemi di informazioni creditizie (Sic) che anche nel 2016 non superano la soglia del 4%, ovvero di quelli rivolti nei confronti del *marketing* che, dopo una forte riduzione nel 2015, raggiunge solo il 3% dei casi nell'anno in esame.

Rimangono sostanzialmente identiche all'anno precedente le percentuali dei vari settori nei quali sono stati divisi i ricorsi con la rilevante eccezione del sensibile incremento percentuale (dal 24 al 31%) di quelli presentati nei confronti degli editori, all'interno dei quali un ruolo preponderante è svolto dai ricorsi rivolti a testate giornalistiche o a motori di ricerca per il riconoscimento – in forma più o meno corretta, come si vedrà – del diritto all'oblio (cfr. par. 21.3).

Si tratta di un incremento significativo, legato senz'altro alle nuove opportunità offerte dalla sentenza della CGUE 13 maggio 2014 C-131/12 (sentenza Google Spain) ma che, probabilmente, costituisce 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, possono comportare sulla sfera personale dell'individuo e nelle sue relazioni con il mondo esterno.

In questo senso, come si vedrà nell'illustrazione di alcuni casi affrontati dal Garante, si rende necessario delimitare con attenzione l'ambito di applicazione del 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 es. quelli legati ad interventi di carattere diffamatorio che, diffusi sul web, vedono aumentata la loro portata negativa e dannosa 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 attesta un certo decremento dei ricorsi: dai 307 del 2015 ai 277 del 2016, pari a circa il 9% su base annua. Anche tale andamento sembra potersi giustificare con la tendenza alla progressiva riduzione di alcuni "filoni" particolarmente attivi negli anni precedenti: si noti, ad es., il sostanziale dimezzamento dei ricorsi nei confronti delle amministrazioni pubbliche e dei concessionari di pubblici servizi, che dai complessivi 20 del 2015 passano ai 12 nel 2016 e, come già in parte accennato, quelli contro gli operatori telefonici e del *marketing*, nonché l'ancor più accentuata diminuzione di quelli presentati contro le società di informazioni commerciali, che dai 23 si riducono a 7.

21.2. *I dati statistici*

Scendendo ad un maggior grado di dettaglio nell'esame dei dati statistici riferiti all'anno 2016 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 (55%), 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. In casi eccezionali, per esigenze di tempestività, è possibile presentare direttamente ricorso al Garante senza rivolgere previamente l'interpello al titolare del trattamento (art. 146, comma 1, del Codice). Anche nel 2016 non sono mancati casi di questo tipo, che hanno consentito all'Autorità di circoscrivere ulteriormente l'ambito di applicazione di tale eccezione. Ad esempio in una prima circostanza è stato ritenuto ammissibile un ricorso proposto in via d'urgenza da un deputato al fine di ottenere la cancellazione dei propri dati anagrafici, dell'indirizzo di residenza e dei suoi recapiti che un giornalista aveva pubblicato sulla propria pagina Facebook dopo averli desunti da una domanda di mediazione da questi proposta nei suoi confronti. Il Garante, condividendo che la pubblicazione di tali dati avrebbe potuto esporre il ricorrente e la sua famiglia ad un pregiudizio imminente ed irreparabile, anche in ragione del ruolo istituzionale svolto, ha ritenuto il ricorso ammissibile, nonostante il mancato inoltro dell'interpello preventivo (provv. 4 febbraio 2016, n. 41, doc. web n. 4774558). Viceversa, in un altro caso, il Garante ha ritenuto non sussistente il pregiudizio imminente ed irreparabile lamentato dal ricorrente che chiedeva la rimozione di alcuni contenuti diffamatori pubblicati sul *blog* del resistente, considerato che si trattava di pubblicazioni risalenti al 2014 e che quindi il lungo periodo di tempo intercorso testimoniava l'inesistenza di un pericolo imminente tale da impedire al ricorrente di presentare previamente l'istanza al titolare del trattamento (provv. 21 settembre 2016, n. 376, doc. web n. 5795994).

Sempre sotto il profilo della tipologia delle decisioni, va sottolineato che, pur rimanendo assai alto – come sopra evidenziato – il numero delle decisioni di non luogo a provvedere, queste registrano comunque una riduzione del 5% rispetto ai due anni precedenti, che trova riscontro in un sensibile incremento delle decisioni di inammissibilità (dall'11 al 18%), da leggersi in parte con riferimento a situazioni contingenti e 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 "maturo" e nella conseguente prospettiva di passaggio dettata dal nuovo regolamento UE.

Non meno significativo è lo sguardo alle principali categorie di titolari del trattamento, sia pubblici che privati, dove si nota immediatamente il superamento, dopo diversi anni, del settore delle banche e società finanziarie (che pure mantiene il considerevole 26%) da parte degli editori che raggiunge il 31% e di cui si è già detto al paragrafo precedente.

A seguire, si rileva anche nell'anno in considerazione un numero significativo di procedimenti attivati nei confronti dei datori di lavoro pubblici e privati. È una casistica che, da un lato, probabilmente, riflette le difficoltà derivanti dalla perdu-

rante crisi occupazionale ma, dall'altro, evidenzia senz'altro il profilo del "nuovo" contenzioso rispetto all'utilizzo delle moderne tecnologie, mettendo in risalto il delicato equilibrio fra tutela della riservatezza dei singoli ed esigenze organizzative del datore di lavoro.

Per il resto, come già in parte riferito, emerge una sensibile diminuzione dei ricorsi relativi all'attività di *marketing* svolta da imprenditori privati, che dal 6% del totale dei ricorsi del 2015 si riducono al 3% nell'anno in esame, e di quelli rivolti contro fornitori di servizi telefonici e telematici (anche qui dal 6 al 3%), una tendenza che, se dovesse essere confermata nei prossimi anni, potrebbe denotare finalmente la "normalizzazione" di un'attività di prospezione commerciale spesso avvertita come particolarmente fastidiosa dall'utenza.

Non superano, poi, il 4% i ricorsi diretti verso altre singole categorie di titolari: amministrazioni pubbliche e concessionari di pubblici servizi (4%); liberi professionisti (3%); strutture sanitarie pubbliche e private (2%); Centrale rischi della Banca d'Italia (1%); associazioni e amministrazioni condominiali (1%).

Infine, pesa per un ulteriore 4% complessivo la restante quota dei ricorsi rivolta contro altri titolari che, singolarmente, non superano la soglia dell'1%. Tra questi meritano menzione quelli presentati contro le parrocchie, generalmente da persone che chiedono di veder annotata nei registri di battesimo la loro volontà di non esser più considerati cattolici, che, per la prima volta dopo diversi anni, non raggiungono la citata soglia minima dell'1%.

21.3. *La casistica più significativa*

In questo paragrafo, oltre ad una breve elencazione, saranno analizzati alcuni fra gli ambiti più significativi attinenti ai ricorsi presentati nell'anno 2016. Peraltro l'elenco, meramente esemplificativo, mira a segnalare alcuni provvedimenti che, in ragione della loro valenza generale, possono fornire utili indicazioni a tutti quei soggetti interessati ad esercitare (nello stesso settore) i diritti tutelati dall'art. 7 del Codice.

Trattamenti in ambito giornalistico

In ambito giornalistico, come accennato, il 2016 è stato caratterizzato da un elevato numero di ricorsi in materia di diritto all'oblio.

I princìpi 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 dell'Autorità.

Fra i casi che occorre menzionare, quali esempi di ricerca di equilibrio fra i contrapposti diritti in gioco, può essere ricordata la decisione assunta il 16 giugno 2016 (provv. n. 267, doc. web n. 5440944) nella quale, pur dovendosi confrontare con il delicato tema legato alla divulgazione di una vicenda giudiziaria conclusasi con una sentenza di condanna ma con il beneficio della non menzione della pena, si è dovuta dichiarare l'infondatezza del ricorso, trattandosi di una sentenza molto recente in relazione alla quale non erano ancora decorsi i termini per l'impugnazione.

Lo scorrere del tempo, però, non può costituire l'unico parametro da prendere a riferimento per l'applicazione del diritto all'oblio, dovendosi contestualmente valutare ulteriori circostanze. Così, ad es., il Garante ha dovuto rigettare in data 6 ottobre 2016 (provv. n. 400, doc. web n. 5690378) la richiesta di rimozione di alcuni url che rimandavano a notizie ritenute dall'interessato estremamente pregiudizievoli considerato che, nonostante il decorso di un significativo periodo di tempo dai fatti (circa 10 anni) la vicenda giudiziaria si era conclusa solo nel 2012, e che la gravità dei reati commessi (corruzione e truffa a danno della sanità regionale della quale il

21

ricorrente è stato un protagonista di rilievo) portava, come indicato anche dalle linee guida del Gruppo Art. 29 (punto 13), a valutare con minor favore le richieste di deindicizzazione.

Ancor più rilevante sotto tale profilo il rigetto (provv. 31 marzo 2016, n. 152, doc. web n. 4988654) della richiesta di un *ex* terrorista volta a far rimuovere da Google gli url che rinviavano ad articoli di stampa, tesi di laurea, atti processuali in cui erano riportati gravi fatti di cronaca che lo avevano visto protagonista tra la fine degli anni 70 e i primi anni 80. L'Autorità, infatti, rilevando che le informazioni di cui si chiedeva la deindicizzazione hanno ormai assunto una valenza storica, avendo segnato la memoria collettiva, ha dichiarato infondato il ricorso, ritenendo sussistente, nonostante il lungo lasso di tempo trascorso dagli eventi, l'interesse pubblico ad accedere ad informazioni relative ad una delle pagine più buie della storia italiana, della quale il ricorrente è stato un vero e proprio protagonista.

Sempre nel nutrito novero di ricorsi contro i motori di ricerca, sono venuti in evidenza diversi casi in cui il bene tutelato non riguardava tanto la corretta applicazione dei diritti di cui all'art. 7 del Codice, quanto piuttosto profili connessi al diritto alla reputazione.

Così in un caso l'Autorità ha dovuto riconoscere che alla richiesta di rimozione di informazioni ritenute inesatte e connesse a contenuti diffamatori caricati sulla piattaforma gestita da YouTube non potevano essere applicati i princìpi in materia di diritto all'oblio, in quanto non sufficientemente provata l'inesattezza dei dati indicati (provv. 11 febbraio 2016, n. 54, doc. web n. 4833107).

Viceversa, in un altro specifico caso il Garante ha accolto la richiesta di deindicizzazione di un articolo pubblicato su un *blog* nel quale erano state riportate vicende asseritamente false, che avevano comportato un grave pregiudizio alla reputazione personale e professionale del ricorrente, considerando che, accertata l'impossibilità di risalire all'autore della pubblicazione, la richiesta dell'interessato di ottenere la deindicizzazione da parte del motore di ricerca rappresentava l'unica possibilità concreta di opporsi al trattamento in questione (provv. 25 febbraio 2016, n. 84, doc. web n. 4881645).

Nel 2016 hanno trovato poi conferma le prime pronunce del Garante sui sistemi automatizzati di ausilio messi a disposizione dai motori di ricerca. In particolare, con la decisione del 27 ottobre 2016, l'Autorità ha disposto la rettifica di uno *snippet* ottenuto effettuando una ricerca per nominativo dell'interessato, considerando il suo contenuto idoneo a fornire non veritiera ricostruzione del fatto rispetto a quanto riportato all'interno dell'articolo di stampa cui esso rinviava (provv. 27 ottobre 2016, n. 444, doc. web n. 5890115).

Con successiva decisione del 24 novembre 2016, il Garante ha parzialmente accolto il ricorso di una persona che lamentava l'accostamento, nell'ambito dei suggerimenti disponibili all'interno della stringa di ricerca risultante dall'utilizzo della funzione di completamento automatico (cd. *autocomplete*), del suo nominativo a termini ritenuti lesivi della propria persona, considerando che effettivamente il riferito accostamento aveva una valenza negativa tale da poter determinare un pregiudizio rilevante per lo stesso interessato (provv. 24 novembre 2016, n. 496, doc. web n. 5905700).

Infine, soprattutto per il suo valore innovativo, merita menzione la decisione assunta in data 11 febbraio 2016 che ha visto per la prima volta coinvolta Facebook quale titolare del trattamento destinataria delle richieste di accesso, cancellazione e blocco dei dati che un *fake account*, illecitamente creato utilizzando la foto postata sul profilo Facebook del ricorrente, avrebbe inviato ai contatti di quest'ultimo. Nel caso di specie, l'Autorità ha preliminarmente riconosciuto la propria competenza, ritenendo applicabile il diritto nazionale nei confronti di Facebook Ireland Ltd., in

ciò facendo riferimento all'interpretazione flessibile del concetto di "stabilimento" di cui all'art. 4, par. 1, lett. *a*) della direttiva 95/46/CE, alla luce dei princìpi affermati dalle sentenze della CGUE Google Spain del 13 maggio 2014 e Weltimmo del 1° ottobre 2015. Nel merito, poi, l'Autorità ha accolto le istanze del ricorrente ordinando a Facebook di comunicare all'interessato tutti i dati che lo riguardavano, anche quelli illecitamente inseriti nel *social network* dal *fake account* (provv. 11 febbraio 2016, n. 56, doc. web n. 4833448).

In ambito giornalistico non sono comunque mancati interventi di carattere più "ordinario", come quello volto a ricordare all'editore di una testata che gli aggiornamenti delle notizie riportate negli articoli conservati nell'archivio storico *online* devono essere effettuati con modalità idonee a rendere immediatamente visibile, sia nel titolo che nel contenuto delle anteprime degli stessi, l'esistenza di sviluppi successivi della vicenda (mediante, ad es., l'inserimento di una nota accanto o sotto al titolo dell'articolo), non potendosi limitare solo ad un'annotazione in fondo all'articolo che risulterebbe visibile solo dopo la lettura dello stesso (provv. 20 ottobre 2016, n. 430, doc. web n. 5690019).

Allo stesso modo, si è dovuto far presente ad altro editore l'esigenza di non indugiare, all'interno di un servizio giornalistico televisivo, su particolari che consentano, anche indirettamente, l'individuazione dell'interessato, laddove ciò non sia essenziale per il raggiungimento della finalità informativa (provv. 3 novembre 2016, n. 454, doc. web n. 5852301).

Trattamenti in ambito lavorativo

Fra i trattamenti effettuati da parte di datori di lavoro pubblico, l'Autorità si è dovuta nuovamente pronunciare sul necessario contemperamento fra esigenze di servizio e tutela della riservatezza dell'interessato. In particolare, con il provvedimento 24 novembre 2016, ha ribadito l'esigenza di rispettare i princìpi di pertinenza e non eccedenza previsti dall'art. 11 del Codice e di indispensabilità, per i dati sensibili, previsti dal successivo art. 22, e ha quindi affermato che l'Ente locale (resistente) doveva astenersi dal riportare all'interno degli ordini di servizio giornalieri ogni informazione idonea a rivelare l'esistenza di una patologia del ricorrente o di una sua limitazione nello svolgimento della prestazione lavorativa parimenti idonea a svelare il suo stato di salute (provv. 24 novembre 2016, n. 497, doc. web n. 5981979).

Con riguardo alle garanzie dovute al lavoratore nell'ambito dell'implementazione delle tecnologie, l'Autorità ha esaminato la richiesta di una *ex* dipendente che chiedeva il blocco del trattamento dei propri dati, effettuato dal titolare attraverso un incrocio tra le informazioni estrapolate dal sistema di apertura della sbarra del parcheggio aziendale confrontate con l'orario di lavoro risultante dal sistema di rilevazione delle presenze e successivamente utilizzate nell'ambito di una contestazione disciplinare conclusasi con il licenziamento della ricorrente. Il Garante, con provvedimento del 3 novembre 2016 (n. 458, doc. web n. 5971482), ha accolto il ricorso ordinando alla resistente di astenersi dall'effettuare ulteriori trattamenti dei dati acquisiti, essendo emerso un comportamento non in conformità ai princìpi di liceità e di correttezza del trattamento previsti dall'art. 11, comma 1, lett. *a*) e 13 del Codice, non essendosi proceduto preventivamente ad informare l'interessata circa la raccolta e le caratteristiche dell'effettivo trattamento dei dati personali e l'eventuale utilizzo degli stessi dati per effettuare controlli su base individuale.

Abbastanza simile, per questi aspetti, la decisione assunta nei confronti di una Fondazione che aveva avuto accesso ai dati relativi all'utilizzo del computer aziendale da parte di un proprio dipendente all'esito di un intervento dovuto a problemi tecnici e che li aveva utilizzati per avviarne una azione di responsabilità culminata con il licenziamento dell'interessato. L'Autorità ha ritenuto, in particolare, che il trattamento posto in essere dal datore di lavoro non potesse considerarsi conforme

agli artt. 3, 11, comma 1, e 13 del Codice e alle disposizioni contenute nello Statuto dei lavoratori; inoltre, sulla base degli atti acquisiti è risultato un contrasto tra la condotta tenuta dal datore di lavoro all'atto della verifica compiuta sul computer della ricorrente e le indicazioni fornite ai dipendenti attraverso l'apposito disciplinare interno sull'utilizzo degli strumenti di lavoro (provv. 12 ottobre 2016, n. 419, doc. web n. 5867780).

Per quanto riguarda gli ulteriori, numerosi ambiti di intervento, merita menzione il provvedimento del 12 maggio 2016 nel quale il Garante ha affrontato un tema particolarmente delicato, relativo alla tutela della riservatezza dell'identità delle madri che al momento del parto si sono avvalse del diritto di non essere nominate. Il caso in esame (provv. 12 maggio 2016, n. 223, doc. web n. 5185339) ha riguardato la richiesta di accedere alla cartella clinica di nascita della ricorrente con annessi i dati della madre biologica. Con il provvedimento adottato il Garante ha accolto l'istanza dell'interessata in relazione ai dati riferiti all'evento della sua nascita, mentre lo ha dovuto dichiarare infondato in ordine alla richiesta di accesso integrale alla cartella clinica con annessi dati della madre biologica (cfr. par. 5.1.5).

In ambito bancario, poi, con il provvedimento del 18 febbraio 2016 il Garante ha ribadito che, ai sensi dell'art. 7 del Codice, è possibile conoscere i dati personali relativi al solo interessato e non anche quelli riferiti a soggetti terzi, quali risultavano essere, nel caso di specie, i dipendenti della banca (provv. 18 febbraio 2016, n. 70, doc. web n. 4842022).

21.4. *I profili procedurali*

Resta da segnalare infine che, al pari di altri strumenti di tutela che l'ordinamento pone a disposizione degli interessati, talvolta anche il ricorso al Garante viene utilizzato con finalità non conformi allo spirito della disciplina di riferimento.

Nel 2016 il Garante, dopo una serie di ricorsi già presentati da un ricorrente nei confronti del medesimo titolare, ha dovuto dichiarare l'inammissibilità di nove ulteriori atti, avendo verificato che essi erano diretti nella quasi totalità dei casi a contestare e far correggere dati di origine contabile e che l'attività si poneva, per numero, frequenza e contenuto nell'ambito di un'attività ritorsiva avviata dal ricorrente nei confronti di quel titolare, realizzata anche attraverso ulteriori atti (parcellizzazione dei pagamenti, inoltro di un numero spropositato di richieste di accesso ai dati, di reclami ed esposti a diverse Istituzioni, ecc.). Tali considerazioni hanno dunque indotto l'Autorità ad inquadrare il predetto comportamento nelle ipotesi distorsive dell'abuso del diritto, richiamato anche dalla giurisprudenza (v. per tutti Cass. civ., III, 18.09.2009, n. 20106) e dell'uso indebito del procedimento, poiché, utilizzando quest'ultimo in modo distorto, si gravava anche ingiustificatamente sull'attività dell'Autorità, con diretti riflessi negativi nei riguardi del pubblico interesse al corretto ed efficiente funzionamento del sistema di tutela approntato dal Codice (provv. 6 ottobre 2016, n. 411, doc. web 5848102).

22 Il contenzioso giurisdizionale

22.1. *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 stesso. In particolare, il citato 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 necessarie; a fronte dei 31 ricorsi notificati nel 2014 e dei 19 nel 2015, nel 2016 sono stati notificati all'Autorità e da questa trattati 12 ricorsi.

Attesa l'importanza dello strumento del ricorso giurisdizionale, posto a disposizione degli interessati e volto alla tutela del diritto alla protezione dei dati personali in alternativa al ricorso presentato in sede amministrativa al Garante, assume sempre maggiore rilevanza l'obbligo – purtroppo non sempre puntualmente adempiuto – per le cancellerie di trasmettere al Garante copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica (art. 154, comma 6). Unitamente alle notifiche dei ricorsi proposti direttamente davanti al giudice, che l'autorità giudiziaria riterrà di effettuare, tale misura potrà consentire al Garante di continuare ad avere 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, comma 5, del regolamento (UE) 2016/679 "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". Per quanto invece riguarda la direttiva (UE) 2016/680, l'art. 47, comma 5, 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".

22.2. *I profili procedurali*

In tema di incompetenza territoriale, il Tribunale di Milano, con ordinanza del 18 gennaio 2016, decidendo su un ricorso proposto da un'articolazione provinciale di un Istituto previdenziale avverso un'ordinanza ingiunzione, si è dichiarato incompetente in favore del Tribunale di Roma, quale tribunale del luogo in cui ha resi-

denza il titolare del trattamento dei dati (art. 10, comma 2, d.lgs. n. 150/2001 come richiamato dall'art. 152 e ss., d.lgs. n. 196/2003), non avendo ravvisato soggettività giuridica in capo alla predetta struttura territoriale dell'Istituto.

In altro caso, il Tribunale di Vibo Valentia ha dichiarato l'incompetenza per materia in favore del Tribunale di Modena o di Bologna, in quanto l'art. 10 citato prevede una competenza speciale a carattere esclusivo del giudice del luogo di residenza o di domicilio del titolare del trattamento, prevalendo tale norma su quella che prevede il foro del consumatore previsto dall'art. 33, lett. *u*), d.lgs. n. 206/2005 (ordinanza 4 gennaio 2016).

Infine, in relazione all'ammontare di una cartella esattoriale relativa ad un'ordinanza ingiunzione emessa dal Garante (18 ottobre 2011, n. 112), il Tribunale di Sondrio ha dichiarato l'incompetenza per valore in favore del Giudice di pace (15 aprile 2016, n. 189), mentre, in altro giudizio relativo ad un'impugnazione di un verbale di contestazione di sanzioni amministrative, il Giudice di pace di Roma si è dichiarato incompetente per materia in favore del Tribunale di Roma (24 settembre 2015, n. 38322).

22.3. *Le opposizioni ai provvedimenti del Garante*

L'anno 2016 ha registrato un leggero decremento nella proposizione delle opposizioni a provvedimenti dell'Autorità, 80, a fronte degli 85 ricorsi del 2015. Di queste, 35 si riferiscono a opposizioni a ordinanze ingiunzioni, in flessione rispetto al 2015 (45). Di seguito si dà conto delle sentenze ritenute di maggior rilievo.

Opposizioni a ordinanze ingiunzioni

Complessivamente il Garante ha avuto notizia di 68 decisioni dell'autorità giudiziaria relative a opposizioni a provvedimenti del Garante, il quale si è sempre costituito in giudizio, tramite l'Avvocatura dello Stato territorialmente competente.

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

Informativa e consenso

Tra le opposizioni alle ordinanze ingiunzioni, 4 decisioni hanno avuto ad oggetto provvedimenti dell'Autorità irroganti sanzioni delle quali due riguardanti la raccolta di dati personali effettuata dai siti internet di alcune aziende in assenza di un'idonea informativa (Trib. Salerno, 10 novembre 2015, 4702; Trib. Vicenza, 16 giugno 2016, n. 1341) e due in merito al consenso (Trib. Como, 4 maggio 2016, n. 606; Trib. Padova, 16 giugno 2015, n. 1812).

In particolare, negli ultimi due casi, il consenso risultava già preselezionato e non poteva considerarsi un'inequivoca manifestazione di volontà dell'interessato pertanto le pronunce, avvalorando la giurisprudenza costante, hanno confermato le valutazioni dell'Autorità e rigettato i ricorsi.

In tema di informativa, inoltre, il giudice ha confermato il provvedimento del Garante in relazione all'illecito trattamento dati compiuto da un laboratorio di analisi il quale, nonostante il cambiamento di compagine sociale e denominazione, aveva mantenuto i vecchi modelli per la raccolta del consenso e dell'informativa (Trib. Savona, 13 aprile 2016, n. 431).

Si segnala, inoltre, la sentenza della Corte di cassazione (11 dicembre 2015, n. 25079) la quale, annullando senza rinvio la decisione del Tribunale di Milano che aveva ritenuto che la fattispecie integrasse l'ipotesi di invio di materiale propagandistico di dimensioni ridotte, di cui al punto 6) del decalogo elettorale (provv. 7

settembre 2005, doc. web n. 1165613), ha ritenuto che, al caso di specie, si applicasse il punto 4) del suddetto catalogo che, nel caso di invio di sms a fini propagandistici, dispone l'obbligatorietà del preventivo consenso e implicitamente della preventiva informativa.

Tre sentenze hanno riguardato l'attivazione di una pluralità di schede telefoniche effettuate da due distinte società nei confronti di singoli interessati in assenza di informativa. In tutti e tre i casi il giudice ha confermato il provvedimento del Garante (Trib. Trento, 14 dicembre 2016, n. 1232; Trib. Brescia, 7 giugno 2016, n. 1747 e Trib. Bergamo, 1 giugno 2016, n. 1870).

Inoltre la Corte di cassazione, su ricorso del Garante, ha avuto modo di pronunciarsi su due casi in relazione alla liceità della raccolta dati effettuata mediante gli *skipass* in dotazione agli sciatori da due distinte società che gestiscono gli impianti di risalita di località sciistiche, confermando le sentenze di primo grado del Tribunale di Sondrio (v. Relazione 2012, p. 247) e annullando le ordinanze ingiunzioni che avevano sanzionato le società per omessa informativa.

In entrambi i casi la Corte ha ritenuto che, in presenza di tornelli dotati di appositi dispositivi a radiofrequenza che si aprono automaticamente all'avvicinarsi di sciatori dotati di etichetta RFID, non fosse necessaria l'informativa, in quanto il meccanismo di riconoscimento a radiofrequenza è azionabile a iniziativa dello sciatore, sicché non ricorre la necessità di una specifica informativa (29 luglio 2016, n. 15901 e 26 gennaio 2016, n. 1422).

In tre sentenze i giudici hanno poi affrontato la questione del termine di 90 giorni entro i quali deve avvenire la notifica agli interessati degli estremi della violazione (art. 14, l. n. 689/1981).

Nei tre casi i giudici hanno respinto i ricorsi promossi, rispettivamente, dal legale rappresentante di una società che aveva attivato una pluralità di schede telefoniche senza rendere la necessaria informativa (di cui si è precedentemente detto), da un Comune al quale era stata notificata un'ordinanza ingiunzione in relazione alla ostensione del nome del titolare sui contrassegni per il transito e la sosta nelle ztl e da una società alla quale è stata contestato l'invio di comunicazioni commerciali in assenza di informativa. Infatti, secondo una costante giurisprudenza, nell'individuazione del *dies a quo* deve ritenersi compreso anche il tempo necessario alla valutazione degli elementi acquisiti all'esito dell'istruttoria (Trib. Bergamo, 1 giugno 2016, n. 1870 e Trib. Bologna, 20 luglio 2016, n. 20767).

Nel terzo caso, riguardante nuovamente l'attivazione di schede telefoniche senza rendere la necessaria informativa da parte di una società, il termine decadenziale dei 90 giorni è stato ritenuto spirato (Trib. Brescia, 8 marzo 2016, n. 673).

Sempre in materia di termini procedimentali, la Corte di cassazione, su ricorso di una società che si era vista confermare dal Tribunale di Marsala un'ordinanza ingiunzione per omessa informativa *ex* art. 13 del Codice per aver effettuato attività promozionale in assenza di informativa, ha ritenuto che la contestazione avanzata dalla ricorrente, in ordine alla decadenza dell'amministrazione dal potere di iniziare il procedimento sanzionatorio per superamento del termine di sei mesi (o nove nei casi complessi) per il completamento dell'istruttoria preliminare, fosse priva di fondamento in quanto, in assenza di un'esplicita previsione di legge, i termini suddetti hanno natura ordinatoria e non perentoria (9 maggio 2016, n. 9316).

Appare utile menzionare inoltre la decisione della Corte di cassazione su ricorso avverso la sentenza del Tribunale di Sondrio che aveva annullato un'ordinanza ingiunzione del Garante, in quanto la farmacia titolare del trattamento aveva collocato il cartello informativo su una parete interna al locale, in maniera non visibile dall'esterno, in data antecedente al provvedimento generale del Garante dell'8 aprile

22

2010. La Corte, annullando la sentenza di primo grado, ha deciso che, anche nel periodo precedente il suddetto provvedimento generale, doveva ritenersi vigente il principio di diritto secondo il quale l'installazione di un impianto di videosorveglianza all'interno di un esercizio commerciale deve formare oggetto di previa informativa (5 luglio 2016, n. 13663).

Notificazione

Tre pronunce hanno affrontato il tema della notificazione prevista dall'art. 37 e ss. del Codice.

In un caso la Cassazione, su ricorso di una casa di cura che si era vista confermare dal Tribunale di Ancona un'ordinanza ingiunzione per omessa notificazione *ex* art. 37 del Codice emessa nei suoi confronti, ha respinto il ricorso, ritenendo che, nel caso di specie, il trattamento di dati riguardanti malattie mentali, infettive e diffusive da parte di esercenti le professioni sanitarie è soggetto all'obbligo di notificazione, in quanto si tratta di insiemi organizzati di informazioni gestiti da strutture anziché da persone fisiche (5 febbraio 2016, n. 8105).

Con riferimento ad un'opposizione proposta da una società che trattava dati biometrici dei lavoratori con finalità di rilevazione delle presenze senza aver presentato la notificazione al Garante e omettendo di richiedere la verifica preliminare, il Tribunale di Cosenza ha confermato il provvedimento dell'Autorità, ritenendo che la verifica preliminare andasse richiesta in quanto le modalità di conservazione centralizzate erano non necessarie e sproporzionate rispetto alle finalità del trattamento, mentre la notifica al Garante era doverosa poiché l'identificazione del soggetto comportava necessariamente la memorizzazione del dato biometrico e l'elaborazione dei dati personali (7 giugno 2016, n. 1258).

In un'altra pronuncia, su impugnazione di una società investigativa sanzionata per aver omesso di notificare al Garante l'effettuazione di trattamenti di geolocalizzazione, l'organo giudicante ha annullato il provvedimento impugnato, non avendo ritenuto le caratteristiche tecniche del sistema di geolocalizzazione idonee a garantire la continuità della localizzazione e l'identificazione delle persone (Trib. Santa Maria Capua Vetere, 23 maggio 2016, n. 2053).

Trattamento dati da parte di soggetti pubblici

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

Tre casi hanno avuto riguardo alla contestazione a diversi comuni del superamento dei tempi massimi di pubblicazione, previsti dalle disposizioni normative di riferimento, di deliberazioni comunali sui rispettivi siti web. Per ognuno l'organo giudicante ha respinto il ricorso e confermato il provvedimento del Garante (Trib. Siena, 25 maggio 2016, n. 401; Trib. Sulmona, 29 giugno 2016, n. 325; Trib. Sciacca, 6 giugno 2016, n. 308).

Nel quarto caso, la Corte di cassazione (5 luglio 2016, n. 13657) ha accolto il ricorso del Garante, annullando la sentenza del Tribunale di Avellino e confermando l'ordinanza ingiunzione emessa nei conforti di un Ente territoriale per aver diffuso dati idonei a rivelare lo stato di salute tramite pubblicazione di graduatorie riguardanti disabili sul proprio sito istituzionale. La Suprema Corte, ribadendo una giurisprudenza costante, ha ritenuto che l'irrogazione della sanzione amministrativa possa essere imputata sia ad una persona fisica sia ad una persona giuridica, quale appunto l'Ente in questione. Ciò in quanto la norma sulla natura personale della responsabilità preesisteva alla normativa sanzionatoria specifica del Codice. Tale norma prevede la configurabilità di una responsabilità solidale della persona giuridica ma non esclude un'autonoma responsabilità della stessa, conformemente all'inquadramento generale sui titolari del trattamento dei dati previsto dallo stesso Codice, in base al quale è considerato titolare del trattamento non solo la persona fisica ma anche la persona giuridica.

In due casi, i giudici, conformemente ad una consolidata giurisprudenza, hanno dichiarato inammissibili i ricorsi proposti rispettivamente da un Comune e da una società assicurativa che hanno impugnato il verbale di contestazione di infrazioni amministrative, atto che implica la sola possibilità di presentare memorie difensive e/o audizioni di fronte all'Autorità, mentre è solo l'eventuale e successiva ordinanza ingiunzione, conclusiva del procedimento sanzionatorio, a poter essere impugnata *ex* art. 152 del Codice (Trib. di Cosenza, 1° marzo 2016, n. 447; Trib. di Foggia, 7 luglio 2016, n. 2207).

Ulteriori casi

Un'altra vicenda ha coinvolto una compagnia telefonica, sanzionata dal Garante per aver utilizzato, per fini promozionali, i dati acquisiti da altre società in assenza di consenso e informativa degli interessati; per tali dati era stato altresì emesso un divieto di trattamento ed era stata applicata la sanzione prevista in relazione alle banche dati di particolare rilevanza e dimensioni.

La Corte di cassazione ha confermato la sentenza di primo grado del Tribunale di Milano, respingendo l'argomentazione della ricorrente che affermava che tra l'illecito di cui all'art. 164-*bis*, comma 2 del Codice e gli altri illeciti non sarebbe configurabile un'ipotesi di cumulo giuridico ma solo un'ipotesi di concorso materiale, ritenendo, invece, che la diversità delle ipotesi contemplate non rilevi solo sul piano quantitativo ma anche su quello qualitativo, poiché il trattamento di dati personali, pur se cospicui, è ben altro dalla gestione e dal trattamento di intere banche dati, assumendo il comportamento sanzionato in quest'ultima ipotesi una rilevanza qualitativa che prescinde dalla mera entità numerica. Pertanto, la Corte ha ritenuto ipotizzabile il concorso degli illeciti amministrativi contestati (17 agosto 2016, n. 17143).

Diritto alla corretta rappresentazione dell'identità personale

Quattro pronunce hanno riguardato la richiesta di deindicizzazione di determinate pagine web proposta dagli interessati nei confronti di un primario motore di ricerca (in tre casi) e del sito fonte delle notizie (nel quarto caso).

In due casi, decidendo su una questione assai controversa ed oggetto di altre impugnazioni non decise entro l'anno, i giudici hanno dichiarato la carenza di legittimazione passiva della società italiana considerata titolare del trattamento poiché quest'ultima aveva "un mero ruolo di consulenza sul settore *marketing* e pubblicitario con riferimento al territorio italiano", mentre i servizi di indicizzazione delle pagine web utilizzate dai motori di ricerca erano gestiti dalla società madre sita all'estero. Nel merito i Tribunali giudicanti hanno respinto i ricorsi, confermando i provvedimenti del Garante, rispettivamente del 4 giugno 2015 n. 335 e 17 settembre 2015, n. 484 (doc. web nn. 4172122 e 4371280), in quanto per entrambi è stato riconosciuto l'interesse pubblico alla notizia, in un caso per il ruolo pubblico del ricorrente, nell'altro per l'attualità temporale dell'informazione, prevalendo tali aspetti sul diritto all'oblio (Trib. Milano, 17 maggio 2016, n. 5640 e 31 maggio 2016, n. 5813).

Nel terzo caso, invece, l'Organo giudicante ha affrontato il tema del bilanciamento tra il diritto alla libertà di informazione e il diritto all'identità personale, stabilendo che, nel caso di specie, inerente la richiesta di deindicizzazione dei dati personali della ricorrente, con specifico riferimento ad un articolo di giornale che dava conto di una vicenda di cronaca che la riguardava, i dati risultavano non pertinenti, non completi e non aggiornati. Il ricorso è stato, pertanto, accolto e il provvedimento del Garante del 31 marzo 2016, n. 156 (doc. web n. 5063807) annullato (Trib. di Milano, 28 settembre 2016, n. 10374).

Un'altra pronuncia ha confermato il provvedimento di non luogo a provvedere del Garante del 30 gennaio 2014, n. 45 (doc. web n. 3033672), emesso a seguito dell'adesione spontanea da parte di un'associazione alla richiesta di anonimizzare un

22

Diritto di accesso ai dati personali

articolo pubblicato sulla propria pagina web, ritenendola una misura tecnicamente idonea ad evitare che le generalità degli interessati fossero rinvenibili attraverso l'uso dei motori di ricerca esterni al sito, respingendo la richiesta di cancellazione delle iniziali e dell'età contenuta nel suddetto articolo a seguito dell'anonimizzazione (Trib. Milano, 2 febbraio 2016, n. 14222).

Tre sentenze hanno riguardato l'esercizio del diritto di accesso.

Una pronuncia, respingendo l'impugnazione avverso il provvedimento del Garante del 27 novembre 2014, n. 550 (doc. web n. 3716398), ha affermato che la richiesta di accesso avanzata da un cliente di conoscere tutti i dati personali relativi ai rapporti intrattenuti con un istituto bancario rientra nell'ambito di applicazione dell'art. 7 del Codice e non del testo unico bancario in quanto quest'ultimo attiene a diverso diritto, con diversa finalità e prescinde dalla presenza di dati personali dei quali si richiede copia (Trib. Pisa, 8 giugno 2016, n. 788).

Altra sentenza (Cass. Civ., 30 maggio 2016, n. 10637) ha dichiarato inammissibile, in quanto "eccentrico" rispetto alla *ratio decidendi*, il ricorso proposto nei confronti della sentenza del Tribunale di Roma che aveva a sua volta dichiarato inammissibile l'impugnazione dell'interessato avverso la pronuncia, pure di inammissibilità, del Garante 7 ottobre 2009 (doc. web n. 1670167) sul ricorso *ex* artt. 145 e segg. del Codice presentato all'Autorità nei confronti di un trattamento effettuato dal Ced del Dipartimento di pubblica sicurezza. Infatti avverso tali trattamenti la tutela presso il Garante non è ammessa nella forma del ricorso, bensì in quella prevista dagli artt. 175, comma 3 e 160 del Codice.

Nell'altro caso, infine, il Tribunale di Trento, annullando il provvedimento del Garante del 18 marzo 2010 (doc. web n. 1715015), aveva a suo tempo ritenuto non vi fosse alcuna prova che i dati bancari di un cliente fossero stati comunicati dall'istituto bancario al coniuge che li avrebbe poi utilizzati in una causa di separazione. La Cassazione ha cassato con rinvio, stabilendo che, di fronte alla contestazione in ordine alla liceità dell'accesso, fondata sulla mancanza di consenso, in quanto effettuato fuori dalle finalità tipiche del rapporto contrattuale, incombeva sulla banca l'onere di dimostrare che l'accesso e il trattamento dei dati fosse ricompreso nella preventiva autorizzazione al trattamento acquisita nel momento genetico del rapporto contrattuale (7 ottobre 2015, n. 20106).

Lavoro

Tre casi hanno avuto ad oggetto il trattamento dei dati personali sul luogo di lavoro.

La prima decisione ha riguardato il ricorso proposto da una società che ha inviato una contestazione disciplinare ad un dipendente relativa ad accessi ad internet non autorizzati effettuati sul luogo di lavoro e per i quali l'interessato aveva chiesto il blocco e la cancellazione.

La Corte di cassazione (20 settembre 2013, n. 18443), aderendo all'orientamento espresso in primo grado dal Tribunale di Palermo, ha confermato il provvedimento del Garante del 2 febbraio 2006 (doc. web n. 1229854), ribadendo che il trattamento, il quale, peraltro, riguardava dati sensibili, era avvenuto in assenza di consenso e informativa circa la possibilità di effettuare controlli sui terminali d'ufficio in violazione dell'art. 4 dello Statuto del lavoratori. In particolare, la Corte ha condiviso le argomentazioni del Garante secondo cui la ricorrente avrebbe potuto dimostrare l'illiceità del comportamento del dipendente, che per svolgere le proprie mansioni lavorative non necessitava di accedere ad internet, limitandosi a provare l'esistenza di accessi indebiti alla rete e i relativi tempi di collegamento, riducendo, così, la quantità di informazioni raccolte allo stretto necessario per la finalità perseguita, secondo quanto previsto anche dalla raccomandazione WP Art. 29, 3 dicembre 1997, n. 3/97 (anonimato su internet). Infine, la Corte ha ritenuto non ricorresse, nel caso di specie, il requisito dell'indispensabilità che consente al datore di

lavoro di trattare dati di natura sensibile senza il consenso dell'interessato per far valere o difendere un diritto in sede giudiziaria.

In altro caso il Tribunale di Napoli, riformando il provvedimento del Garante del 18 settembre 2014, n. 420 (doc. web n. 3560798), ha stabilito che l'impianto di videosorveglianza installato in un istituto scolastico, seppur attivato con finalità esclusive di sicurezza e prevenzione in orario non lavorativo, ricade nell'ambito di applicazione dell'art. 4 dello Statuto dei lavoratori, essendo, da questo punto di vista, la semplice comunicazione alle Rsu effettuata dall'istituto stesso insufficiente a consentire l'istallazione del sistema di videosorveglianza (23 febbraio 2016, n. 1612).

Analogamente, il Tribunale di Firenze ha confermato il provvedimento del Garante del 16 febbraio 2012, n. 63 (doc. web n. 1892377), che aveva dichiarato illecito il trattamento effettuato da una Azienda sanitaria locale, concretatosi nell'installazione di un impianto di videosorveglianza nell'area del sistema di rilevazione delle presenze dei dipendenti, in assenza di accordo con le rappresentanze sindacali. L'organo giudicante ha ritenuto che il fatto che i soggetti ripresi non siano immediatamente riconoscibili non comporta di per sé l'inapplicabilità del Codice potendo, nel caso di specie, essere identificati in un momento successivo; ha anche affermato che l'inquadramento dell'orologio marcatempo integri di per sé un controllo a distanza dell'attività dei lavoratori, conformemente a quanto sostenuto dal Garante, in linea con una consolidata giurisprudenza (11 gennaio 2016, n. 717).

La Corte di cassazione, con sentenza del 30 maggio 2016, n. 1140, ha chiuso una complessa vicenda relativa al provvedimento del Garante del 5 dicembre 2001 (doc. web n. 40405) – poi integrato in data 30 gennaio 2002 (doc. web n. 1084563) – con i quali, in relazione alla procedura della RAI di ottenere i dati personali degli acquirenti di apparecchi radiotelevisivi da parte dei rivenditori degli stessi al fine di ottenere nuovi abbonamenti, ha segnalato all'Agenzia delle entrate, in quanto titolare del trattamento, e alla RAI, responsabile del trattamento, la necessità di interrompere la raccolta e il trattamento dei dati. La Corte ha confermato il provvedimento del Garante, condividendo pienamente le argomentazioni poste a fondamento della decisione di primo grado e stabilendo che, a seguito della soppressione del registro di carico e scarico di apparecchi radioelettrici e della stipula della convenzione aggiuntiva del 1999, la RAI doveva considerarsi responsabile e non titolare del trattamento; pertanto, la raccolta di informazioni presso i rivenditori aveva violato le istruzioni ricevute dall'Amministrazione, mentre l'Agenzia a sua volta aveva consentito lo svolgimento di attività di trattamento non delegabili alla RAI. Contrariamente a quanto sostenuto dalla Corte d'appello, che aveva riformato la sentenza di primo grado stabilendo che la delibera del Garante aveva violato il principio di tipicità dell'atto amministrativo, in quanto aveva inteso esercitare un sostanziale potere di proibizione inquadrabile nell'art. 31, lett. *l*) e non nell'art. 31, lett. *b*) o *c*) della l. n. 675/1996, il giudice di legittimità ha poi affermato che il provvedimento impugnato si sostanziava in una manifestazione di intento non direttamente autoritativo ed interdittivo ma persuasivo dell'opportunità di desistere dall'iniziativa e di cessare il trattamento dei dati così raccolti.

In altro caso la Corte di cassazione ha respinto il ricorso di una società che aveva effettuato attività di *telemarketing* per conto di altra azienda e che era stata condannata in primo grado dal Tribunale di Roma per trattamento illecito in relazione al fenomeno delle cd. telefonate mute. La Corte ha confermato il provvedimento del Garante del 6 dicembre 2011, n. 674 (doc. web n. 1857326) ribadendo che la modalità di trattamento prescelta è da ritenersi contraria al principio di correttezza di cui all'art. 11 del Codice, in quanto diretta ad ottimizzare il successo delle chiamate passate agli operatori facendo ricadere il rischio e il disagio della cd. chiamata

muta sui soli destinatari. Inoltre, il giudice di legittimità ha respinto anche l'ulteriore argomento proposto dalla ricorrente secondo cui il consenso non è richiesto per chi è iscritto negli elenchi degli abbonati ai servizi di telefonia e non ha esercitato il diritto di opposizione, ritenendo che, in linea con la direttiva europea sulla protezione dei dati personali poi recepita dal Codice, il sistema di *opt-out* è previsto per le sole chiamate con operatore, non, invece, per quelle automatizzate, per le quali è invece necessario il consenso (4 febbraio 2016, n. 2196).

In altro caso la Corte di cassazione, conformemente a quanto deciso in primo grado dal Tribunale di Milano avverso l'impugnazione del provvedimento del Garante del 25 marzo 2008 (doc. web n. 1507012), ha stabilito che l'obbligo di conservazione dei tabulati telefonici per finalità di accertamento e repressione dei reati da parte di un operatore del settore è di 24 mesi e non di 48, come affermato dal ricorrente che si era visto negare un'istanza di accesso ai dati tardiva e che riteneva che il termine più ampio dovesse applicarsi anche ai delitti per i quali era previsto l'arresto in flagranza, tesi che secondo l'organo giudicante non trova fondamento nel Codice (28 gennaio 2015, n. 16259).

22.4. *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.

23 L'attività ispettiva e le sanzioni

23.1. *La programmazione dell'attività ispettiva*

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

Nel 2016 sono state effettuate 282 ispezioni. L'attività ispettiva viene organizzata sulla base di programmi elaborati secondo linee di indirizzo stabilite dall'Autorità con delibere che individuano gli ambiti del controllo e gli obiettivi numerici da conseguire. Le linee generali della programmazione dell'attività ispettiva vengono quindi rese pubbliche attraverso il sito web del Garante e, sulla base dei criteri così fissati, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo e istruisce i conseguenti procedimenti (provv.ti 10 marzo 2016, n. 107, doc. web n. 4807706 e 28 luglio 2016, n. 327, doc. web n. 5408359).

La programmazione relativa al 2016 ha previsto che l'attività ispettiva fosse indirizzata, tra gli altri, ai seguenti settori:

- operatori telefonici, per la verifica dei trattamenti di dati personali effettuati in relazione alle attività di *marketing* telefonico espletate mediante *call center*, anche attraverso l'utilizzo di sistemi automatizzati, nonché con l'invio di sms promozionali;
- società di carattere multinazionale, con riferimento ai trattamenti relativi al trasferimento di dati personali, nell'ambito di flussi intra-gruppo, nei Paesi non appartenenti all'Unione europea, avvalendosi delle garanzie contenute nelle *Binding corporate rules* (Bcr);
- centri di assistenza fiscale (Caf), con riferimento ai trattamenti di dati personali dei contribuenti svolti da tali soggetti, per la verifica del rispetto delle misure organizzative e di sicurezza adottate nell'ambito della trasmissione della dichiarazione dei redditi precompilata;
- titolari di grandi banche dati pubbliche (ad es., Agenzia delle entrate, Inps), per la verifica di alcuni trattamenti di dati personali effettuati dagli stessi, anche in relazione alla dichiarazione dei redditi precompilata;
- soggetti commerciali vari, in relazione alle attività di *marketing* telematico effettuate tramite l'utilizzo della posta elettronica e di internet;
- società private, con riferimento al trattamento di dati genetici, finalizzati allo studio del dna umano, effettuati da un istituto privato di ricerca genetica e biomedica.

Come specificato nel successivo par. 23.3, nel periodo di riferimento sono state altresì effettuate, in altri settori, verifiche:

- sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;
- sull'adempimento dell'obbligo di notificazione da parte di soggetti, pubblici e privati, individuati mediante raffronto con il registro generale dei trattamenti;

- sulla liceità e correttezza dei trattamenti di dati personali, con particolare riferimento al rispetto dell'obbligo di informativa, alla pertinenza e non eccedenza nel trattamento, alla libertà e validità del consenso – nei casi in cui questo è necessario –, nonché alla durata della conservazione dei dati nei confronti di soggetti, pubblici o privati, appartenenti a categorie omogenee.

Nello svolgimento delle descritte iniziative ispettive è prioritario rivolgere l'attenzione ai profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate.

23.2. *La collaborazione con la Guardia di finanza*

L'Autorità si avvale della preziosa collaborazione della Guardia di finanza per lo svolgimento dell'attività di controllo. In merito all'ambito di collaborazione, si fa rinvio a quanto riferito in dettaglio nelle precedenti edizioni (cfr. Relazione 2009, p. 240 e ss.), evidenziando ancora una volta la meritoria attività svolta dal Nucleo speciale *privacy*, che ha provveduto direttamente a effettuare gli accertamenti delegati, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti.

Considerati gli ottimi risultati raggiunti nel rapporto di collaborazione, ormai ultra decennale, tra il Garante e la Guardia di finanza e al fine di tenere conto delle nuove sfide tecnologiche nonché del rilievo sempre maggiore che il contesto internazionale avrà nelle istruttorie – anche a seguito delle recenti modifiche apportate al quadro normativo europeo in materia (cfr. regolamento (UE) 2016/679) – è stato stipulato, nel mese di marzo 2016, un nuovo protocollo d'intesa con la Guardia di finanza.

Il nuovo protocollo prevede, dal punto di vista strategico, che il Garante possa avvalersi di personale specializzato della Guardia di finanza per la conduzione di ispezioni congiunte con altre autorità estere (l'introduzione del nuovo regolamento europeo in materia di dati personali, infatti, renderà tale necessità sempre più frequente).

Da un punto di vista più strettamente operativo, invece, il nuovo protocollo garantisce: una sempre maggiore semplificazione dei flussi documentali tra l'Ufficio e il Nucleo speciale *privacy* (attraverso l'uso sistematico di strumenti di trasmissione telematici); l'introduzione di modalità di verifica *online* di possibili violazioni alla normativa in materia di protezione dei dati personali (attraverso l'esame diretto di siti web, senza necessità di ispezioni *in loco*); un coinvolgimento stabile del Nucleo frodi telematiche della Guardia di finanza in attività ispettive o di analisi ad alto contenuto tecnico/informatico.

Sulla base della prassi operativa ormai consolidata, le informazioni e i documenti acquisiti nell'ambito degli accertamenti dal Corpo sono trasmessi all'Autorità per le successive verifiche in ordine alla liceità del trattamento e al rispetto dei princìpi previsti dalla legge.

Nei casi in cui sono emerse sospette violazioni penali o amministrative, la Guardia di finanza ha provveduto a informare l'autorità giudiziaria competente e ad avviare i procedimenti sanzionatori amministrativi mediante la redazione della "contestazione", in conformità alla l. 24 novembre 1981, n. 689.

Grazie alla sinergia ormai collaudata con il Nucleo speciale *privacy* della Guardia di finanza, il Garante può realizzare sofisticate attività di controllo, integrando così le iniziative ispettive svolte direttamente dal competente dipartimento dell'Autorità e consentendo l'effettuazione, efficace e tempestiva, di tutte le verifiche *in loco* che si rendono necessarie per garantire il rispetto della protezione dei dati personali su tutto il territorio nazionale.

In tale quadro, riveste una particolare importanza l'attività di formazione effettuata dal personale della Guardia di finanza al fine di approfondire la conoscenza delle disposizioni del Codice e dei provvedimenti dell'Autorità. Al riguardo, con il Nucleo speciale *privacy* e il Nucleo speciale frodi tecnologiche della Guardia di finanza, è stata organizzata la visita studio della delegazione dell'Autorità di protezione dei dati della Repubblica del Kosovo sullo specifico tema "*Data protection in the law enforcement sector*"; la speciale iniziativa formativa si è svolta nell'ambito dell'assistenza denominata TAIEX (*Technical Assistance and Information Exchange Instrument*), finanziata dalla Commissione Europea e indirizzata ai Paesi candidati e potenziali candidati, per fornire assistenza relativamente alla trasposizione della legislazione dell'Unione europea nella legislazione nazionale dei Paesi beneficiari.

23.3. *I principali settori oggetto di controllo*

Oltre a quanto già riportato al par. 23.1, le ispezioni effettuate dall'Autorità nel 2016 hanno riguardato le seguenti categorie di titolari del trattamento:

- società esercenti l'attività di *car sharing,* in relazione ai trattamenti di dati personali effettuati nei confronti della propria clientela – con particolare riferimento al trattamento di dati volti a rilevare la posizione geografica di persone o oggetti mediante una rete di comunicazione elettronica – ed ai dati raccolti attraverso l'utilizzo di siti web, nonché ad eventuali trattamenti di profilazione effettuati;
- società operanti nel settore del commercio di autoveicoli, anche per la verifica dei trattamenti di dati personali sensibili degli acquirenti diversamente abili, la cui acquisizione è finalizzata alla richiesta di tassazione agevolata ed all'eventuale comunicazione ad officine autorizzate per l'adattamento dei veicoli;
- società di web *marketing,* con riferimento ai trattamenti di dati personali relativi ai servizi offerti dalle stesse alla propria clientela (web *marketing, e-mail marketing, mobile marketing, lead generation, direct mailing, market profiling*);
- agenzie di lavoro interinale, in relazione alle attività di profilazione effettuate dai cd. *head hunter* per la ricerca di personale altamente qualificato;
- soggetti esercenti l'attività di investigazione privata, in relazione all'accertamento di eventuali acquisizioni illecite di dati personali;
- società operanti nel settore dell'intermediazione creditizia o della concessione di prestiti, in relazione ai trattamenti di dati personali effettuati nei confronti della propria clientela, con particolare riferimento alle eventuali attività di profilazione o *marketing*, alla comunicazione a terzi, nonché ai casi in cui i dati sono trattati nell'ambito dei sistemi di informazioni creditizie per definire il profilo o la personalità della clientela o per finalità di controllo sulla referenza creditizia;
- società costruttrici di autoveicoli, per la verifica dei trattamenti di dati personali effettuati dalle concessionarie del marchio, per la fornitura di servizi di assistenza e vendita di autoveicoli, anche con riferimento ai *software* gestionali in uso alle suddette concessionarie e ai siti internet alle stesse riferibili, nonché in relazione all'eventuale trattamento di sensibili degli acquirenti o a quelli effettuati per finalità di profilazione della clientela;
- società che offrono servizi di assistenza tecnica di apparati di telefonia mobile e di prodotti informatici, con specifico riferimento ai trattamenti

effettuati sui dati personali raccolti, nell'ambito delle attività di "assistenza tecnica o recupero dati", dagli apparati telefonici/informatici della clientela;
- società che offrono servizi di "gioco a distanza", con specifico riguardo al trattamento dei dati personali dei giocatori raccolti nell'ambito dei servizi *online,* anche in riferimento all'eventuale profilazione degli interessati, alla comunicazione a terzi dei dati personali trattati o all'eventuale trasferimento degli stessi in altri Paesi, anche non appartenenti all'Unione europea;
- soggetti operanti nel settore della "gestione del debito", in merito ad alcune criticità emerse nelle modalità di raccolta dei dati personali degli utenti tramite siti internet e in relazione ad alcune segnalazioni ricevute dal Nucleo speciale *antitrust* della Guardia di finanza.

Oltre all'elenco prospettato, sono stati effettuati altresì ulteriori specifici controlli nei confronti di titolari del trattamento per esigenze istruttorie connesse alle segnalazioni, ai reclami e ai ricorsi pervenuti all'Autorità.

In relazione a quanto emerso dagli accertamenti effettuati, sono state formulate numerose proposte di adozione di provvedimenti inibitori e/o prescrizioni per conformare il trattamento alla legge, a fronte delle quali l'Autorità, come riportato nel prossimo paragrafo, ha adottato alcuni provvedimenti particolarmente significativi per i cittadini.

23.4. *I provvedimenti adottati dall'Autorità a seguito dell'attività ispettiva*

Attraverso le ispezioni l'Autorità svolge un'incisiva attività istruttoria che può essere finalizzata, a seconda del caso, 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 definendo le misure necessarie da prescrivere 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).

L'attività ispettiva si realizza comunque nell'ambito di un procedimento amministrativo di controllo all'esito del quale, ove vengano accertate illiceità, l'Autorità è tenuta ad adottare i necessari provvedimenti per rendere il trattamento conforme alla legge e a contestare le sanzioni eventualmente rilevate.

Con riferimento all'anno 2016, tra i provvedimenti più rilevanti adottati dal Garante sulla base degli elementi istruttori acquisiti in sede ispettiva si segnalano, in particolare, i provvedimenti con i quali il Garante ha:
- adottato un parere sul nuovo schema di provvedimento del Direttore dell'Agenzia delle entrate per l'accesso alla dichiarazione precompilata da parte del contribuente e degli altri soggetti autorizzati (provv. 7 aprile 2016, n. 157, doc. web n. 4916838; cfr. par. 4.6);
- dichiarato illecito e vietato il trattamento dei dati personali, utilizzati da una società di telefonia per attività promozionale effettuata attraverso il *tele-*

marketing, senza aver preventivamente acquisito il consenso dagli interessati (provv. 22 giugno 2016, n. 275, doc. web n. 5255159; cfr. par. 10.3);
- dichiarato illecito e vietato il trattamento dei dati personali, utilizzati da una società di formazione per attività promozionale effettuata tramite l'invio di sms, senza avere, anche in questo caso, acquisito il relativo consenso dagli interessati (provv. 27 ottobre 2016, n. 437 doc. web n. 5727908; cfr. par. 10.3).

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.

23.5. *L'attività sanzionatoria del Garante*

23.5.1. Le violazioni penali e procedimenti relativi alle misure minime di sicurezza

Nell'anno 2016, in relazione alle istruttorie effettuate, sono state inviate all'autorità giudiziaria 53 segnalazioni di violazioni penali, di cui:
- trentacinque per la mancata adozione delle misure minime di sicurezza;
- sei per violazioni della l. n. 300/1970 (Statuto dei lavoratori), ora punite come reato dall'art. 171 del Codice;
- cinque per trattamento illecito dei dati;
- due per inosservanza di un provvedimento del Garante;
- cinque in relazione ad altre violazioni penali.

Come dimostrano i dati sopra riportati, sono ancora 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 e che dovrebbero essere stati oramai "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 i dati personali degli interessati alla possibilità che vi abbiano accesso persone non autorizzate e che siano effettuati trattamenti non consentiti, incidendo così negativamente sul naturale affidamento degli interessati nei confronti del titolare del trattamento.

Sotto il profilo procedurale, nel caso in cui venga rilevata una violazione di una o più delle misure minime di sicurezza (specificatamente previste dal disciplinare tecnico sulle misure di sicurezza All. B. al Codice), in base al disposto dell'art. 169, comma 2, del Codice, il Garante impartisce una prescrizione alla persona individuata come responsabile della predetta violazione e, successivamente, verificato il ripristino delle misure violate, ammette il destinatario della prescrizione al pagamento del quarto del massimo della sanzione prevista (pari a 30.000 euro). L'adempimento alla prescrizione ed il pagamento della somma vengono comunicati all'autorità giudiziaria competente per le valutazioni in ordine all'estinzione del reato.

In questo ambito appare opportuno richiamare la sentenza della Corte di cassazione penale (sentenza n. 1986/2015) che ha affrontato, respingendola, la questione di legittimità costituzionale del sopra citato art. 169 del Codice, in riferimento agli artt. 2, 3, 21, 24 e 25 della Costituzione. Nella motivazione si legge che "non sussiste, infatti, alcun contrasto di tale disposizione con gli art. 3 e 24 Cost., perché rientra in generale nella piena discrezionalità del legislatore la fissazione dell'ammontare dell'oblazione ai fini dell'estinzione del reato, come avvenuto, attraverso il richiamo all'art. 162, comma 2-*bis*, in ragione di euro 30.000".

Nella stessa sentenza la Suprema Corte afferma che la responsabilità penale "è stata, del resto, positivamente accertata dalla Guardia di finanza nel corso delle indagini preliminari, attraverso l'accertamento diretto della mancata designazione del-

23

l'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.

Appare opportuno rilevare che anche nel 2016 si è avuta un'incidenza non trascurabile dell'accertamento di violazioni penali relative allo Statuto dei lavoratori, connesse, nella maggior parte dei casi, all'installazione di sistemi di videosorveglianza in assenza delle garanzie previste dall'art. 4, comma 2, l. n. 300/1970. La disciplina prevista dallo Statuto e relativa all'utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4) e al divieto di indagini sulle opinioni ai fini dell'assunzione (art. 8), si configura quale parte integrante delle disposizioni del Codice (artt. 113 e 114), espressamente sanzionata dall'art. 171.

Sul punto occorre evidenziare che la materia ha subito profonde modifiche a seguito dell'adozione del d.lgs. 14 settembre 2015, n. 151 (cd. *Jobs Act*). Le modifiche apportate attengono sia alla parte sostanziale della disciplina del controllo a distanza dei lavoratori (art. 4, l. n. 300/1970) sia a quella sanzionatoria (art. 171 del Codice).

In questo contesto, si sottolineano le specifiche modifiche apportate al quadro sanzionatorio, ovvero alla nuova formulazione dell'art. 171 del Codice, nella parte in cui si prevede che "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 mancanza di accordo, previa autorizzazione della Direzione del lavoro; al comma 2, che la disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal 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.

Tale sanzione resta invece con riferimento all'utilizzo di impianti audiovisivi e di altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, qualora installati in assenza dell'accordo sindacale o, in alternativa, dell'autorizzazione della Direzione territoriale del lavoro.

Meno chiara risulta invece l'inclusione del comma 2, art. 4, dello Statuto nell'area coperta dalla sanzione penale prevista dal nuovo art. 171; tale disposizione sottrae dall'ambito di applicazione delle disposizioni di cui al comma 1 (e quindi esonera dalla necessità di accordo/autorizzazione), gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e gli strumenti di registrazione degli accessi e delle presenze".

È, infine, sottratto alla valutazione del giudice penale il contenuto del comma 3 dell'art. 4 che prevede che "le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196".

Da ciò ne deriva che la mancata informazione ai lavoratori circa le modalità di uso degli strumenti e di effettuazione dei controlli rientra invece nell'orbita delle valutazioni di competenza dal punto di vista della legittimità del trattamento dei dati personali.

23.5.2. Le sanzioni amministrative

Nell'anno 2016 sono stati avviati n. 2.339 nuovi procedimenti sanzionatori amministrativi.

L'accertamento delle violazioni amministrative previste dal Codice può essere effettuato:

- dal personale dell'Ufficio addetto all'attività ispettiva a cui, sulla base di quanto previsto dall'art. 156, comma 9, del Codice, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, è attribuita la qualifica di ufficiale o agente di polizia giudiziaria;
- da chiunque rivesta, nell'esercizio delle proprie funzioni, la qualifica di ufficiale o agente di polizia giudiziaria, in base a quanto previsto dall'art. 13 della legge 24 novembre 1981, n. 689.

La specifica disciplina legislativa di settore (art. 13 della l. n. 689/81) prevede che "Gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro possono, per l'accertamento delle violazioni di rispettiva competenza, assumere informazioni e procedere a ispezioni di cose e di luoghi diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica. All'accertamento delle violazioni punite con la sanzione amministrativa del pagamento di una somma di denaro possono procedere anche gli ufficiali e gli agenti di polizia giudiziaria".

I procedimenti sanzionatori iniziano, pertanto, con la contestazione in relazione ad istruttorie effettuate direttamente dall'Autorità ma anche sulla base di accertamenti effettuati autonomamente da corpi dello Stato quali la Guardia di finanza, i Carabinieri, la Polizia di 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", non delimitando la possibilità di effettuare attività di accertamento solo da parte del Garante, risulta estremamente efficace, considerata l'amplissima platea delle categorie di soggetti tenuti all'osservanza delle disposizioni del Codice.

La prioritaria esigenza di assicurare una uniformità di giudizio e di interpretazione è peraltro assicurata dal Codice che espressamente affida al solo Garante il compito dell'applicazione delle sanzioni in tutti i casi nei quali, a seguito dell'accertamento, il contravventore, non avvalendosi della possibilità di definire il procedimento con il pagamento entro sessanta giorni dalla notifica del doppio del minimo della sanzione, decida di proseguire il procedimento medesimo inviando alla stessa Autorità scritti difensivi o chiedendo l'audizione. In tutti questi casi è infatti il Garante a decidere in ordine all'applicazione della sanzione adottando l'atto finale dell'ordinanza ingiunzione, quantificandone l'importo, o l'archiviazione.

23

Le violazioni in relazione alle quali sono stati avviati procedimenti sanzionatori nel 2016 hanno riguardato:

- la mancata comunicazione agli interessati, da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico, di violazioni di dati personali (cd. *data breach*) degli stessi (n. 1.817);
- la mancata comunicazione al Garante, da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico, di violazioni di dati personali (cd. *data breach*) del contraente o di altra persona (n. 1);
- il trattamento illecito – art. 162, comma 2-*bis* (n. 203);
- l'omessa o inidonea informativa – art. 161 (n. 200);
- l'omessa o incompleta notificazione – art. 163 (n. 37);
- l'omessa adozione delle misure minime di sicurezza di cui all'art. 33 del Codice – art. 162, comma 2-*bis* (n. 33);
- l'omessa informazione o esibizione al Garante – art. 164 (n. 32);
- l'inosservanza di un provvedimento del Garante – art. 162, comma 2-*ter* (n. 11);
- la conservazione di dati di traffico telefonico e telematico per un tempo superiore a quello stabilito dall'art. 132 del Codice – art. 162-*bis* (n. 3);
- la violazione di disposizioni del Codice in relazione a banche dati di particolari rilevanza o dimensioni – art. 164-*bis*, comma 2 (n. 2).

Un approfondimento merita il dato relativo alle 1.818 sanzioni amministrative contestate in relazione alla mancata comunicazione di violazioni di dati personali (cd. *data breach*) al Garante e agli interessati. Tali sanzioni sono riconducibili, infatti, ad un rilevante *data breach* occorso ad un importante operatore nazionale, fornitore di servizi di comunicazione elettronica accessibili al pubblico, il quale non ha provveduto a comunicare tale evento né al Garante (ai sensi dell'art. 32-*bis,* comma 1, del Codice, che prevede: "In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione al Garante"), né ai 1.817 interessati direttamente coinvolti dalla violazione dei propri dati personali (ai sensi dell'art. 32-*bis,* comma 2, del Codice, il quale prevede: "Quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza del contraente o di altra persona, il fornitore comunica anche agli stessi senza ritardo l'avvenuta violazione"). I suddetti comportamenti omissivi sono stati, pertanto, sanzionati dal Garante in applicazione, rispettivamente, dei commi 1 e 2, dell'art. 162-*ter,* del Codice.

I procedimenti sanzionatori definiti nell'anno 2016 con provvedimento di ordinanza adottato dall'Autorità, relativamente a violazioni contestate (anche) negli anni precedenti al 2016 e non definite all'epoca attraverso il pagamento spontaneo in misura ridotta da parte del contravventore, sono stati 355. Di questi, 175 hanno comportato l'applicazione di una sanzione (per un ammontare complessivo di somme ingiunte pari a 993.200 euro) e 180 si sono invece conclusi con l'archiviazione in quanto la parte ha potuto dimostrare nel procedimento di non aver commesso la violazione contestata o che la violazione non era ad essa imputabile.

Tra le ordinanze adottate, quelle più significative hanno riguardato:

- sistemi di autenticazione informatica basati su tecniche di *strong authentication* di cui al provvedimento generale del 17 gennaio 2008 (doc. web n. 1482111). Tra le tecniche di *strong authentication* previste dal citato provvedimento, poste a presidio dell'effettuazione di trattamenti di dati di traffico telefonico e telematico conservati per finalità di accertamento e repressione dei reati, quella che deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato, si sostanzia anche nel necessario utilizzo di

sistemi di riconoscimento biometrico per il controllo delle aree ad accesso selezionato (ordinanza-ingiunzione 25 febbraio 2016, n. 81, doc. web n. 5431626);

- ambito interpretativo della responsabilità solidale nel caso del titolare del trattamento dei dati/trasgressore soggetto all'altrui vigilanza ai sensi dell'art. 6, comma 2, l. n. 689/1981. Tale responsabilità deve essere rilevata alla luce del disposto di cui all'art. 29, comma 5, del Codice che impone al titolare del trattamento di vigilare, anche tramite verifiche periodiche attestate da atti puntualmente individuati nella fase istruttoria del procedimento amministrativo, sull'osservanza delle istruzioni impartite al responsabile, ove, peraltro, l'estemporaneità della condotta oggetto di contestazione e la sua conseguente impossibilità di essere impedita da parte del trasgressore non può essere circoscritta al singolo caso, ma deve essere valutata dall'Autorità a fronte di un'attività istruttoria mirata; la qualificazione della carenza di attività di direzione e vigilanza è riconducibile alla previsione della responsabilità solidale di cui all'art. 6, comma 2, della l. n. 689/1981 (ordinanza-ingiunzione 10 novembre 2016, n. 464, doc. web n. 5890728);
- distinzione fra poteri ispettivi ai sensi degli artt. 157 e 158 del Codice. I poteri previsti dall'art. 157 del Codice (richiesta di informazioni ed esibizione di documenti) configurano un'attività di tipo collaborativo (basata su una dialettica del tipo "domanda-risposta") condotta nei confronti del titolare, del responsabile, dell'interessato e anche di terzi. Ben diversi sono i poteri ispettivi di tipo autoritativo, disciplinati dagli artt. 158 e 159 del Codice, con accessi ai luoghi del trattamento, agli archivi e alle banche dati indipendentemente dalla volontà del soggetto ispezionato. Le garanzie previste dall'art. 159 del Codice, nella parte in cui dispone (comma 3) che "Gli accertamenti, se effettuati presso il titolare o il responsabile, sono eseguiti dandone informazione a quest'ultimo o, se questo è assente o non è designato, agli incaricati. Agli accertamenti possono assistere persone indicate dal titolare o dal responsabile", operano esclusivamente per questa seconda categoria di accertamenti, come ben può desumersi dal contenuto letterale delle disposizioni di tale articolo, le quali fanno esclusivamente riferimento alle modalità di svolgimento degli accessi, delle verifiche e delle rilevazioni previsti dall'art. 158 del Codice e non anche delle semplici richieste di informazioni ed esibizioni di documenti di cui all'art. 157 (ordinanza-ingiunzione 13 luglio 2016, n. 308, doc. web n. 5751157);
- utilizzo della posta elettronica certificata per la notifica della contestazione della violazione amministrativa alle imprese costituite in forma societaria. In base all'art. 14, comma 3, l. n. 689/1981, la notificazione della contestazione di violazione amministrativa può essere effettuata anche da un funzionario dell'amministrazione che ha accertato la violazione, con le modalità previste dal codice di procedura civile il quale all'art. 149-*bis*, comma 1, prevede che "la notificazione può eseguirsi a mezzo posta elettronica certificata, anche previa estrazione di copia informatica del documento cartaceo". Deve inoltre considerarsi che la notifica telematica prevede una sequenza caratterizzata dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna le quali contengono, rispettivamente, la prova dell'avvenuta spedizione di un messaggio di posta elettronica certificata e la prova che detto messaggio sia effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario, certificando il momento della consegna. Tale sequenza, congiuntamente all'obbligo per le imprese costituite in forma

societaria di dotarsi della posta elettronica certificata (art. 16, d.l. n. 185/2008, convertito con modificazioni dalla l. n. 2/2009), conferisce valore legale alle comunicazioni elettroniche nei confronti di tali imprese (ordinanza-ingiunzione 13 luglio 2016, n. 308, doc. web n. 5751157);

- la persona fisica assume la qualità di titolare del trattamento di dati effettuato per ragioni di giustizia. L'ordinanza ha preso in esame l'attività di un consulente tecnico dell'autorità giudiziaria, che nell'ambito dei propri incarichi consulenziali ha raccolto dati personali e li ha organizzati in un archivio gestito autonomamente. Il Garante ha rilevato che, nella sua attività, il consulente ha trattato tali dati personali oltre il termine stabilito dall'autorità giudiziaria e anche per finalità diverse da quelle stabilite dall'art. 47 del Codice (ragioni di giustizia) assumendo, in tale ultima ipotesi, il ruolo di autonomo titolare del trattamento. Il consulente ha inoltre messo a disposizione di numerosi soggetti, fra cui anche alcuni giornalisti, atti giudiziari acquisti nel corso della sua attività, causando un'indebita comunicazione di dati giudiziari. Il Garante ha sanzionato il consulente per avere utilizzato banche dati di particolare rilevanza e dimensioni in violazione delle norme in tema di informativa, consenso, autorizzazione del Garante (ordinanza-ingiunzione 31 marzo 2016, n. 148, doc. web n. 4858951).

L'ammontare dei pagamenti effettuati nell'anno 2016 da parte dei soggetti nei cui confronti sono stati avviati procedimenti sanzionatori amministrativi è risultato complessivamente pari a 3.289.896 euro di cui:

- 2.324.440 euro riscossi in conseguenza della definizione in via breve;
- 432.976 euro 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;
- 150.000 euro per la definizione, in sede amministrativa, dei procedimenti relativi alla mancata adozione delle misure minime di sicurezza;
- 382.480 euro 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 vincolati unicamente per l'esercizio della attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

24 Le relazioni comunitarie e internazionali

24.1. *La riforma del quadro giuridico europeo in materia di protezione dei dati*

Nel 2016 si è chiuso l'*iter* di approvazione del nuovo quadro normativo europeo in materia di protezione dei dati, il cd. pacchetto protezione dati. Come ampiamente illustrato nella Relazione 2015, il pacchetto comprende un regolamento generale sulla protezione dei dati (2016/679) e una direttiva sulla protezione dei dati in materia di polizia e giustizia (2016/680); il primo diverrà pienamente esecutivo il 25 maggio 2018, mentre la seconda dovrà essere recepita nell'ordinamento nazionale entro il 6 maggio 2018 (per quanto concerne l'impatto della riforma sulla normativa in essere e sulle attività dell'Autorità cfr. *infra* e cap. 1).

24.2. *La cooperazione tra autorità di protezione dati nell'UE: il Gruppo Art. 29*

Il pacchetto di riforma UE

Il Gruppo Art. 29 ha cominciato, con congruo anticipo rispetto all'effettiva adozione del cd. pacchetto protezione dei dati, a lavorare sull'impatto della riforma e sul processo di transizione verso il nuovo quadro normativo che troverà applicazione a partire dal 25 maggio 2018.

In quest'ottica, già a febbraio, il Gruppo ha adottato, insieme al programma di lavoro 2016-2018 (WP 235, doc. web n. 5774811), un piano d'azione che individua come priorità per il 2016 (WP 236, doc. web n. 6109526): l'organizzazione amministrativa interna del Comitato per la protezione dei dati (e, in particolare, le risorse IT, le risorse umane e il *budget*); la preparazione della cooperazione tra le autorità (*One-Stop-Shop*) e del meccanismo di coerenza; l'adozione di linee guida per aiutare titolari e responsabili del trattamento a orientarsi nel nuovo quadro normativo; l'attività di comunicazione relativa al futuro Comitato per la protezione dei dati e del regolamento sulla protezione dei dati. Seguendo il piano d'azione, il Gruppo (attraverso i lavori dei suoi sottogruppi e le sei riunioni plenarie) ha così iniziato a fornire le prime indicazioni sulle novità normative previste dal regolamento, lavorando già su alcune linee guida, e ad approfondire lo studio delle disposizioni del regolamento relative alla cooperazione tra le autorità e al futuro ruolo del Comitato. Nello svolgimento di tali attività, il Gruppo ha prestato molta attenzione al contesto nel quale opera e, in quest'ottica, ha cercato di aprirsi al confronto con i diversi *stakeholder* sia attraverso l'organizzazione di eventi su temi specifici (FabLab 26 luglio 2016, doc. web n. 6120299), sia attraverso lo strumento della consultazione pubblica su alcune linee guida adottate.

Nel 2016 sono stati adottati, in particolare, le linee guida sui responsabili della protezione dei dati (RPD, in inglese "*Data Protection Officer* - DPO), il documento sulla designazione dell'autorità capofila (*lead authority*) e le linee guida in materia di diritto alla portabilità. I tre documenti – che portano in allegato specifiche *frequently asked questions* (FAQ) per facilitarne l'applicazione pratica – sono stati pubblicati sul sito del Gruppo 29 il 13 dicembre 2016 e sono stati aperti a consultazione pubblica fino al 15 febbraio 2017.

Linee guida sui Responsabili della protezione dei dati

Le linee guida sugli RPD (*Guidelines on Data Protection Officers* (DPOs) WP243 e relative FAQ doc. web n. 5930287) mirano a chiarire le disposizioni del regolamento (artt. 37 e ss.) con particolare riferimento ai requisiti e agli obblighi del RPD, al fine di favorire l'osservanza della normativa da parte di titolari e responsabili del trattamento e facilitare il lavoro degli stessi responsabili della protezione dei dati.

Si tratta di un documento significativo soprattutto per i Paesi che, come il nostro, con l'entrata in vigore del regolamento, si trovano per la prima volta ad affrontare l'introduzione di una figura determinante per l'applicazione del nuovo quadro di regole, obbligatoria per i soggetti pubblici e – in ambito privato – per gli specifici trattamenti previsti dall'art. 37 del regolamento.

Le linee guida si soffermano in particolare sull'interpretazione delle ipotesi – previste dal regolamento – di nomina obbligatoria del RPD, ne descrivono i requisiti, le competenze e la posizione anche rispetto al necessario ruolo di indipendenza all'interno della struttura (pubblica o privata) in cui opera. Forniscono altresì raccomandazioni sulle migliori pratiche da seguire, basate, ove possibile, sull'esperienza acquisita negli Stati membri dell'UE.

Autorità capofila

Un altro tema di particolare novità del nuovo quadro europeo sulla protezione dei dati riguarda la designazione della autorità capofila (*lead authority*) che deve rivestire il ruolo di cd. sportello unico nei cd. trattamenti transnazionali ove cioè, ai sensi dell'art. 4 del regolamento, 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.

Come nel caso del RPD, il Gruppo ha ritenuto necessario adottare linee guida (WP244 doc. web n. 6109704 e relative FAQ, doc. web n. 6109687) con l'intento di supportare titolari o responsabili del trattamento nella corretta individuazione dell'autorità competente al fine di evitare controversie e garantire un'attuazione efficace del regolamento.

Il documento si sofferma tra l'altro, sulla questione 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*, della contitolarità del trattamento.

Linee guida in materia di diritto alla portabilità

Le linee guida sul diritto alla portabilità (WP 242, doc. web n. 6058842 e relative FAQ, doc. web n. 6058857) illustrano le peculiarità del nuovo diritto previsto dall'art. 20 del regolamento distinguendolo da quello di accesso ai dati personali. Si prevede che tale diritto possa essere esercitato sia in presenza di un terzo titolare a cui trasferire i dati, sia in sua assenza e si precisa che i dati personali oggetto del diritto (ad es. "i dati personali che lo riguardano forniti a un titolare del trattamento" da un interessato) non sono solo quelli consapevolmente forniti dall'interessato ma anche quelli "osservati" (quali, ad es., il numero di volte in cui si ascolta un brano di una *playlist*) con esclusione di quelli che derivano da un'analisi condotta dal titolare (quali, ad es., profili, *scoring*, etc. che pure costituiscono dati personali ma possono solo formare oggetto di istanze di accesso).

Il parere si sofferma sulle modalità di esercizio del diritto: verifica identità, tempi di risposta, tutela del segreto aziendale, formato interoperabile che consenta un effettivo riutilizzo dei dati, misure di sicurezza necessarie per la trasmissione dei dati, etc.

Con riferimento agli elementi di novità del regolamento, il Gruppo ha avviato una riflessione anche sul *Data Protection Impact Assesmment* (cd. DPIA) previsto dall'art. 35 del regolamento, in vista dell'adozione di uno specifico parere come previsto dal piano d'azione.

Cooperazione tra autorità e meccanismo di coerenza

Nell'ambito delle attività svolte per la predisposizione del futuro quadro giuridico, molta attenzione è stata dedicata all'analisi dei nuovi obblighi di cooperazione previsti in capo alle autorità di protezione dei dati (cui il regolamento si riferisce utilizzando la più ampia espressione "autorità di supervisione") e degli strumenti che potranno essere utilizzati per rendere tale cooperazione più fluida ed efficace. Partendo dall'analisi testuale delle disposizioni contenute nel Capo VII, il Gruppo ha elaborato alcuni documenti interpretativi e alcune linee guida interne in tema di assistenza reciproca, operazioni congiunte e sportello unico, predisponendo anche modelli comuni per la cooperazione che verranno messi alla prova nel corso del 2017 al fine di individuare eventuali modifiche e integrazioni (comunicato stampa WP29 16 dicembre 2016, doc. web n. 6119901).

Sempre al fine di favorire l'applicazione piena delle norme previste dal regolamento a partire dal maggio 2018, il Gruppo ha avviato una riflessione sul complesso tema delle sanzioni e delle condizioni generali per la loro applicazione previste dall'art. 83 e, attraverso un'analisi dei compiti attribuiti al futuro Comitato europeo per la protezione dei dati, su un suo possibile regolamento interno. Con l'aiuto del Garante europeo per la protezione dei dati (che metterà a disposizione del futuro Comitato il segretariato), si è lavorato anche alla predisposizione della struttura informatica necessaria per garantire un'agevole cooperazione tra le autorità di supervisione e tra le stesse e il Comitato.

Revisione della direttiva *e-Privacy* (2002/58/EC)

Il Gruppo ha reso, a luglio, il parere sulla valutazione e revisione della direttiva 2002/58 relativa alla vita privata e alle comunicazioni elettroniche nell'ambito della consultazione pubblica avviata dalla Commissione europea a ridosso dell'adozione del pacchetto di riforma sulla protezione dei dati. Nel parere (WP 240, doc. web n. 5774868), il Gruppo concorda con la Commissione con riguardo alla necessità di avere un quadro di norme specifiche per il settore delle comunicazioni elettroniche ma precisa che lo strumento in materia di *e-Privacy* deve completare e specificare le norme del regolamento generale sulla protezione dei dati senza che vi sia, tra gli stessi, un rapporto *lex specialis/generalis*. Scopo primario della direttiva 2002/58/CE è proteggere la segretezza e la sicurezza delle comunicazioni (inclusi i dati generati da sistemi di comunicazione che non sono dati personali) e fornire protezione in tale ambito anche alle persone giuridiche. Lo stesso livello di protezione deve essere garantito anche alle nuove forme di comunicazione, ad es. VOIP e *app* mobili e, a fronte della varietà dei soggetti a cui la direttiva si rivolge (ad es., le norme sulle comunicazioni indesiderate si rivolgono a qualunque soggetto e non ai *provider* di reti o servizi), occorre che gli articoli del nuovo strumento siano chiari nell'esplicitare i destinatari degli obblighi previsti e, allo stesso tempo, che le definizioni di tali destinatari siano rese più chiare e in grado di racchiudere tutti i *provider* interessati (*wired* o *wireless*, privati o pubblici, di internet *voice*, *chat*, ecc.). Riguardo alle comunicazioni indesiderate occorre mantenere un approccio tecnologicamente neutro che preveda che tutte le comunicazioni indesiderate (indipendentemente dal mezzo usato) siano soggette al consenso preventivo dell'interessato.

I principali aspetti su cui il WP 29 si è soffermato sono:

- ambito di applicazione: dopo un'attenta definizione dei servizi, appare necessario che tutti i soggetti che li eroghino (anche con modalità/canali differenti) rientrino nell'ambito di applicazione della nuova direttiva/regolamento, specialmente con riferimento al divieto di raccogliere dati relativi alle comunicazioni (art. 5.1). Il parere prevede, in ordine all'art. 5.1, due possibili eccezioni: 1. per garantire la trasmissione del servizio; 2. per garantirne la sicurezza (bloccando eventuali *malware* che il *provider* possa con certezza individuare);

- applicazione del 5.3: assicurare che la disposizione sia tecnologicamente neutra specificando le eccezioni per il *tracking*, ma anche per i *cookie* analitici;
- unificare le disposizioni in materia di dati di traffico e di localizzazione (attuali artt. 6 e 9) e ampliarne lo scopo visto che si tratta di metadati che necessitano di adeguate misure di protezione indipendentemente dal titolare del trattamento. Tali dati devono rientrare nell'ambito dell'art. 5.1 ma anche in questo caso alcune eccezioni specifiche sono previste, in particolare nel caso di *privacy by design* e anonimizzazione;
- eliminazione delle disposizioni sul *data breach* ormai assorbite dal GDPR;
- divieto di trattamenti ulteriori senza consenso (in particolare per la creazione di liste di contatti indipendentemente dalla piattaforma utilizzata: telefono, *e-mail*, indirizzi Skype, etc.) e *opt-in* per tutti i tipi di comunicazioni indesiderate;
- direttiva o regolamento: per evitare un'applicazione differente tra gli stati membri, il parere suggerisce che anche il nuovo strumento in materia di *e-Privacy* sia un regolamento.

Dati personali e nuove tecnologie

Anche al di fuori dalla valutazione delle specifiche novità del regolamento e della proposta di direttiva *e-Privacy*, il Gruppo ha continuato la sua attività di approfondimento con riferimento all'impatto delle nuove tecnologie sulla protezione dei dati.

Sono stati oggetto di attenzione i temi del tracciamento di posizione effettuato tramite reti Wi-Fi e *bluetooth*, e del cd. *do-not-track*.

Inoltre, con lettera 28 ottobre 2016 (doc. web n. 6119829) il Gruppo si è rivolto a Yahoo! a seguito del furto di dati a opera di *hacker* relativi a milioni di suoi utenti, che ha avuto ampia eco nei mezzi di informazione internazionali. Le autorità di protezione dati hanno manifestato la loro preoccupazione e invitato Yahoo Inc. a dedicare risorse adeguate per comprendere e risolvere una violazione di dati senza precedenti e notificarne gli effetti agli interessati coinvolti.

Con due lettere, rispettivamente del 27 ottobre (doc. web n. 6119793) e del 16 dicembre 2016 (doc. web n. 6119924), il Gruppo si è invece rivolto a WhatsApp in merito all'annunciata condivisione dei dati dei loro utenti con Facebook. Con la prima lettera, il Gruppo ha sollecitato WhatsApp affinché non si procedesse a tale condivisione in assenza delle necessarie garanzie giuridiche, in particolare con riferimento agli obblighi di informativa agli interessati (senza i quali il consenso al trattamento non può dirsi validamente prestato), e i meccanismi offerti agli utenti per esercitare il loro diritti.

Con la seconda lettera, con la quale ha preso atto dell'impegno di WhatsApp di astenersi dal condividere i dati relativi agli utenti europei con Facebook e le società ad essa affiliate allo scopo di migliorare i prodotti di Facebook e la relativa pubblicità, il Gruppo ha reiterato le preoccupazioni relative a possibili condivisioni di dati per finalità diverse e sottolineato che, al di là dell'intervento congiunto del Gruppo Art. 29, WhatsApp resta obbligato a fornire riscontro alle diverse richieste di informazioni pervenute dalle autorità di protezione dati nazionali (cfr. cap. 13).

Sempre nel settore delle nuove tecnologie, il Garante è stata delegato dal Gruppo Art. 29 a seguire i lavori del *Working Group* C-ITS sui sistemi di trasporto intelligenti attivato dalla Commissione in vista di un contributo del Gruppo nel corso del 2017.

Protezione dei dati in ambito finanziario

Il Garante ha proseguito nel ruolo di coordinatore del sottogruppo *Financial Matters* incaricato di approfondire le diverse questioni legate all'applicazione della disciplina sulla protezione dei dati nel settore finanziario.

Su impulso di tale sottogruppo, il Gruppo Art. 29 ha continuato a lavorare sul tema dello scambio automatizzato tra Stati di dati a fini fiscali, in particolare con

riferimento ai *Common reporting standard* dell'OCSE che si propongono quale modello globale per lo scambio di informazioni tra amministrazioni fiscali ai fini della lotta all'evasione (v. Relazione 2014, p. 177). Il lavoro di approfondimento ha portato all'adozione di una lettera indirizzata all'OCSE (doc. web n. 6119860) con la quale il Gruppo ha espresso le sue preoccupazioni riguardo alle forti ripercussioni sui diritti fondamentali di meccanismi che comportano significative operazioni di trattamento e scambio dei dati. Si tratta del secondo intervento del Gruppo in tale settore motivato dalla necessità di approntare un sistema di scambio di informazioni rispettoso dei princìpi di protezione dati, anche alla luce del nuovo quadro normativo europeo di protezione dei dati e della più recente giurisprudenza della CGUE (v. in particolare il caso Schrems). Nella lettera, il Gruppo esprime la volontà di aprire un dialogo attivo con gli organi competenti dell'OCSE in uno sforzo comune volto ad individuare meccanismi efficaci che, nel perseguire il legittimo interesse della lotta all'anti-evasione, non espongano i diritti degli individui ad interferenze sproporzionate.

Il Gruppo si è altresì occupato del regolamento della Banca centrale europea (BCE) sulla raccolta di dati granulari sul credito e di dati sul rischio creditizio (cd. Anacredit) che istituisce una nuova base di dati contenente informazioni dettagliate sui prestiti bancari a livello individuale nell'area dell'euro a supporto di varie funzioni delle banche centrali, fra cui il processo decisionale della politica monetaria e la vigilanza macro-prudenziale.

A tal proposito il Gruppo ha predisposto un modello di lettera che le autorità nazionali di protezione dati hanno inviato alle rispettive banche centrali, nonché un'ulteriore lettera, indirizzata alla BCE, al fine di ottenere alcuni chiarimenti volti a valutare l'impatto del progetto Anacredit sulla protezione dei dati.

Il Gruppo ha inoltre continuato l'approfondimento degli strumenti di anti-riciclaggio e lotta al finanziamento del terrorismo, oggetto di una cospicua attività normativa a livello UE. È stata discussa la nuova proposta della Commissione sull'uso del sistema finanziario ai fini di riciclaggio e finanziamento del terrorismo (cd. 5ª direttiva anti-riciclaggio).

La proposta (del 5 luglio 2016), volta ad emendare la 4ª direttiva anti-riciclaggio a poco più di un anno dalla sua pubblicazione, mira a rafforzare la lotta al riciclaggio e al finanziamento del terrorismo anche attraverso la totale accessibilità al pubblico dei registri dei titolari effettivi, l'interconnessione dei registri, nonché la messa a disposizione delle autorità competenti di maggiori informazioni. Nella plenaria di dicembre il Gruppo ha adottato una lettera rivolta alla Commissione europea (doc. web n. 6119883) con la quale ha sottolineato che gli scambi di ingenti quantità di dati personali, seppure comprensibilmente necessari ai fini di lotta all'evasione fiscale e al finanziamento del terrorismo, devono essere accompagnati da strumenti di tutela adeguati che garantiscano in particolare la sicurezza dei dati e che i dati raccolti non siano adoperati per fini ulteriori. Inoltre, riguardo alla creazione di un registro dei titolari effettivi di prodotti e servizi finanziari (cd. *beneficial ownership*) volto a facilitare le attività di indagine delle autorità competenti, il Gruppo sottolinea l'inopportunità di un accesso universale a tale registro e la necessità che nell'individuazione dei criteri di accesso a tale registro sia garantito il rispetto dei princìpi di necessità, finalità e proporzionalità.

Il Gruppo ha continuato il lavoro di approfondimento sulla ratifica dell'Accordo FATCA (la legislazione USA antievasione fiscale *off shore*, *Foreign Account Tax Compliance Act*) nei vari Stati membri. In particolare è proseguita l'attività di verifica della qualità delle misure di implementazione di FATCA e della proporzionalità dello scambio di informazioni tra UE ed USA, attraverso l'invio di un questio-

nario a tutti i membri del WP29 su alcune problematiche aperte, anche in vista di future azioni congiunte di *enforcement*. Da una preliminare analisi sulle prime risposte ricevute è emerso che ancora pochi Paesi hanno una concreta esperienza con FATCA e che la maggior parte di essi non sta ancora inviando informazioni FATCA all'IRS (*Internal Revenue Service*), riscontrando problemi nella trasmissione dei dati.

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 princìpi di protezione dati, specie alla luce del nuovo quadro europeo.

È stato infine avviato uno studio sulla profilazione in ambito finanziario, in via preliminare raccogliendo informazioni su casi nazionali ed esperienze in merito delle varie autorità di protezione dati e procedendo ad un'analisi delle disposizioni normative rilevanti introdotte dal regolamento, anche in vista delle linee guida sulla profilazione che il Gruppo Art. 29 intende adottare nel corso del 2017.

Pubblicazione di dati personali per scopi di trasparenza nel settore pubblico

Alla luce del rilievo che sta acquisendo il tema della trasparenza nel settore pubblico in alcuni Paesi membri dell'UE, il Gruppo ha adottato il parere 2/2016 sul tema, fornendo indicazioni pratiche, raccomandazioni ed esempi di migliori prassi ai legislatori e alle Istituzioni competenti degli Stati membri (ovvero quelle che si occupano del contrasto alla corruzione, della prevenzione dei conflitti di interesse e di altri adempimenti in materia di trasparenza, oltre che alle autorità per la protezione dei dati) affinché l'interesse pubblico alla trasparenza sia bilanciato con la protezione dei dati, qualora iniziative, anche legislative, in questo ambito necessitino della diffusione di informazioni relative a persone fisiche (WP 239, doc. web n. 5774856).

In particolare, partendo da nota giurisprudenza della CGUE (v. sent. 20 maggio 2003, Rundfunk, cause riunite C-465/00, C-138/01 e C-139/01 e sent. 9 novembre 2010, Volker e Markus Schecke, cause riunite C-92/09 e C-93/09), il parere richiama i legislatori nazionali al necessario rispetto dei princìpi di proporzionalità, minimizzazione e qualità dei dati, fornendo anche alcuni esempi di trattamenti che non possono essere considerati, in linea di massima, proporzionati tra cui: la pubblicazione di dati personali relativi ai familiari di una figura pubblica (nominativi, informazioni di contatto, indirizzi, ecc.); la pubblicazione di dati personali relativi a dichiarazioni sull'assenza di conflitti di interesse rese da soggetti operanti nel settore pubblico con responsabilità esclusivamente amministrative, tenuto conto del fatto che questi soggetti non rivestono cariche elettive o ministeriali; la pubblicazione *online* di informazioni di dettaglio relative ai redditi individuali e ai compensi percepiti da soggetti che rivestono qualifiche di livello elevato nell'amministrazione (ad es., dirigenti generali), quali il codice identificativo o fiscale, le relazioni finanziarie per esteso, informazioni dettagliate ricavate da denunce dei redditi o dai cedolini stipendiali, informazioni bancarie o indirizzi privati, numeri di telefono personali o *account* personali di posta elettronica.

Smart borders

Il Gruppo ha adottato il 30 settembre una lettera in relazione al nuovo pacchetto di proposte in tema di *Smart borders* presentato dalla Commissione europea ad aprile 2016 (doc. web n. 6119952). Il WP29 ha indirizzato la lettera al Consiglio e Parlamento UE, accompagnata da un dettagliato allegato, evidenziando gli aspetti più problematici dal punto di vista della protezione dei dati: il rispetto dei princìpi di necessità e proporzionalità con riferimento alle misure previste dal pacchetto (in particolare la creazione di una nuova banca dati *entry-exit*); l'interoperabilità con altri sistemi informativi (VIS, SIS, Eurodac, etc.); l'accesso a fini di *law enforcement*;

l'uso di dati biometrici e i periodi di conservazione proposti (5 anni in luogo dei 180 giorni prefigurati dall'originaria proposta del 2013).

Misure di sorveglianza e garanzie essenziali per il rispetto dei diritti

A seguito della sentenza della CGUE 6 ottobre 2015 (causa C-362/14, Maximillian Schrems v. Data Protection Commissioner) che, nell'invalidare la decisione 2000/250 con cui la Commissione europea aveva dichiarato adeguata la protezione offerta dal sistema *Safe Harbor* (v. Relazione 2015, p. 161), ha toccato il tema della sorveglianza indiscriminata per finalità di *intelligence* e sicurezza nazionale, il Gruppo Art. 29 ha continuato il proprio lavoro su tale argomento (avviato già nel 2014, dopo le prime indiscrezioni relative allo scandalo cd. *datagate*, v. Relazione 2014, p. 176) individuando, nel documento di lavoro 1/2016, le "garanzie" essenziali che, per gli ordinamenti europei, devono essere rispettate affinché eventuali limiti al diritto alla vita privata e alla protezione dei dati personali posti per finalità di sorveglianza possano essere considerati leciti (WP 237, doc. web n. 5774832). Il documento illustra, in particolare, gli elementi che consentono di verificare la sussistenza negli ordinamenti (anche di Paesi terzi, al fine di verificarne la loro "adeguatezza" per consentirvi i trasferimenti di dati personali dall'UE) di quattro specifiche garanzie: 1) il trattamento deve essere fondato su regole chiare, precise ed accessibili; 2) deve essere dimostrato che le interferenze siano "necessarie e proporzionate" rispetto allo scopo legittimo che intendono perseguire; 3) deve sussistere un sistema di supervisione che garantisca un controllo indipendente; 4) l'interessato deve avere a disposizione rimedi effettivi nel caso di violazioni. Per definire il documento, il Gruppo ha analizzato la pertinente giurisprudenza della CGUE relativa agli artt. 7, 8 e 47 della Carta dei diritti fondamentali e quella della Corte EDU relativa all'art. 8 della Convenzione del 1950 (un elenco della stessa è contenuto nell'allegato al WP237).

Trasferimento dati all'estero

Il tema dei trasferimenti di dati verso Paesi terzi ha impegnato, nel 2016, buona parte dell'agenda del Gruppo Art. 29. Per effetto della già citata sentenza Schrems (causa C-362/14 del 6 ottobre 2015, v. Relazione 2015, p. 161), la Commissione europea ha dovuto infatti negoziare un nuovo accordo che consentisse il trasferimento dei dati verso gli Stati Uniti e rivedere le proprie decisioni in materia di adeguatezza e di clausole contrattuali *standard*. Si è pervenuti così, da un lato, all'adozione dell'Accordo EU-USA "Scudo *Privacy*" (*Privacy Shield*) e alla decisione (UE) 2016/1250 con cui la Commissione europea ha dichiarato adeguato il quadro giuridico dallo stesso previsto per i trasferimenti di dati personali effettuati dall'UE verso titolari e responsabili statunitensi che si siano autocertificati nel sistema "Scudo" e, dall'altro, all'adozione delle decisioni di esecuzione (UE) 2016/2295 e 2016/2297 del 16 dicembre 2016 con cui sono state modificate le precedenti decisioni in materia di adeguatezza e clausole contrattuali tipo (*standard contractual clauses*). Il Gruppo Art. 29 ha seguito con attenzione tali attività fornendo indicazioni attraverso dichiarazioni e pareri che, per diversi aspetti, la Commissione ha accolto.

L'Accordo *Privacy Shield*

La Commissione europea ha presentato la prima bozza di decisione di adeguatezza relativa all'Accordo EU-USA per il trasferimento di dati personali cd. Scudo *Privacy* nel febbraio 2016. Il 13 aprile 2016, il Gruppo Art. 29 ha adottato il parere 1/2016 sulla bozza di decisione e sull'allora disponibile testo dell'Accordo, composto da diversi documenti e lettere, allegati alla decisione di adeguatezza della Commissione, con cui le autorità statunitensi e gli organismi di controllo competenti descrivono la legislazione di settore e si impegnano a verificare il rispetto dell'Accordo medesimo (WP 238, doc. web n. 5774844). Nel riconoscere i miglioramenti rispetto al precedente Accordo *Safe Harbour*, il Gruppo ha tuttavia individuato alcuni aspetti critici e invitato la Commissione a rivedere, per quanto possi-

24

bile, Accordo e decisione di adeguatezza. In particolare, tre i punti di maggiore "preoccupazione" che dovevano essere meglio affrontati dall'Accordo: l'assenza del principio di conservazione dei dati per il tempo strettamente necessario alle finalità per le quali gli stessi sono raccolti e successivamente trattati; il rischio di una raccolta indiscriminata di dati personali per finalità di sorveglianza e l'indipendenza e i poteri dell'*Ombudsperson* (il meccanismo previsto dall'Accordo per garantire un controllo sulle attività dell'*intelligence*).

Con riferimento agli aspetti commerciali, il parere sottolinea la necessità di ottenere alcuni chiarimenti su altri aspetti del *Privacy Shield* non pienamente in linea con la disciplina europea di protezione dei dati. Tra i principali: l'assenza di riferimenti espliciti a come i responsabili del trattamento debbano applicare i princìpi elencati nello *Shield* (salva la vincolatività delle indicazioni dei titolari del trattamento contenute nel contratto); l'assenza di garanzie nel caso di decisioni automatizzate e di un generale diritto di opporsi per motivi legittimi; l'adeguatezza del principio sulla "scelta" e alcune criticità legate alle sue concrete modalità di applicazione; il pericolo di trasferimenti ulteriori verso Paesi terzi che consentano di eludere le tutele adeguate previste dalla direttiva e l'assenza di un chiaro richiamo al rispetto del principio di finalità nel trasferimento dei dati; i limiti ampi all'esercizio delle richieste di accesso; l'effettività dell'*enforcement* e dei meccanismi di tutela dei diritti; alcuni aspetti specifici della disciplina prevista per il trattamento dei dati dei lavoratori e di quella per finalità di ricerca farmaceutica o per prodotti sanitari (in questo ambito, ad es., l'esclusione dei dati codificati dall'applicazione dell'Accordo comporta la necessità di chiarire che questi dati sono dati personali che per essere trasferiti necessiteranno di una differente base giuridica). Il Gruppo ha altresì sottolineato la necessità di rivedere l'Accordo al momento dell'applicazione del regolamento generale sulla protezione dei dati.

Dopo il parere del Gruppo Art. 29, la Commissione europea ha rinegoziato, anche se solo per alcuni punti, l'Accordo e ha modificato la propria decisione di adeguatezza, ripresentandola a luglio 2016. La nuova versione dell'Accordo e, soprattutto, la decisione di adeguatezza (UE) 2016/1250 hanno meglio definito il complessivo quadro normativo di riferimento nel quale si inserisce il *Privacy Shield,* consentendo un'interpretazione maggiormente conforme alla direttiva riguardo alcuni passaggi poco chiari (v. ad es., i passaggi relativi al rispetto del principio di finalità e conservazione dei dati per il periodo strettamente necessario al perseguimento delle medesime finalità – par. 21-23 – o gli esempi relativi ai trattamenti per finalità compatibili contenuti nella nota n. 1 dell'allegato II).

Con una dichiarazione del 26 luglio 2016, il Gruppo Art. 29, pur riconoscendo i miglioramenti introdotti, ha mantenuto alcune perplessità (in particolare in ordine all'assenza di garanzie specifiche nel caso di trattamenti automatizzati e di un generale diritto di opporsi per motivi legittimi e rispetto all'effettiva indipendenza dell'*Ombudsperson* e alle garanzie fornite dall'Ufficio del direttore dell'*intelligence* nazionale-ODNI in ordine alla raccolta massiva e indiscriminata di dati personali) e ha considerato il primo riesame comune del funzionamento dello Scudo come un momento essenziale per valutare la solidità e l'efficacia dell'Accordo (cfr. dichiarazione WP 29 sulla decisione di adeguatezza, doc. web n. 6109001).

Al fine di contribuire a rendere operativo l'Accordo, il 13 dicembre 2016, il Gruppo Art. 29 ha poi adottato due brevi guide rivolte alle imprese che vogliono utilizzare il sistema *Privacy Shield* per il trasferimento di dati personali a società che operano negli USA come titolari del trattamento o come responsabili del trattamento e agli interessati che intendano presentare reclami legati all'applicazione dell'Accordo.

Le FAQ per le imprese (WP 245, doc. web n. 6109610) contengono i *link* ai principali documenti relativi all'Accordo e spiegano come verificare quali società statunitensi siano parte dello stesso e cosa è necessario fare prima di trasferire i dati. Rispetto a tale ultimo punto, il documento distingue tra il caso in cui l'importatore sia un titolare del trattamento (nel qual caso, prima di tutto, andrà ricercata la base giuridica che consente il trasferimento dei dati e verificato il rispetto dei princìpi fondamentali della protezione dei dati – minimizzazione, finalità, proporzionalità, qualità, etc.) e quello in cui l'importatore sia un responsabile del trattamento (con la conseguente necessità di sottoscrivere un contratto con cui il titolare lo designi responsabile del trattamento ai sensi dell'art. 17 della direttiva 95/46/CE e individui modalità e limiti del trattamento che lo stesso dovrà effettuare per suo conto).

Le FAQ rivolte agli interessati (WP246, doc. web n. 6109757) spiegano in breve cosa è il *Privacy Shield*, quali garanzie possono derivare dallo stesso e come presentare un eventuale reclamo per trattamenti effettuati da società che sono autocertificate nel sistema e che hanno ricevuto i dati personali da società stabilite in EU.

Decisioni di adeguatezza e clausole contrattuali tipo (SCC)

Tenuto conto che la CGUE ha considerato invalido l'art. 3 della decisione di adeguatezza relativa al *Safe Harbour* in quanto limitativo dei poteri delle autorità di protezione dei dati previsti dall'art. 28 della direttiva 95/46/CE (cfr. sentenza Maximillian Schrems, causa C-362/14, parr. 99 e ss.) e che disposizioni contenenti analoghi limiti erano contenute in tutte le decisioni di adeguatezza adottate dalla Commissione europea e nelle decisioni relative alle clausole contrattuali *standard* (decisioni 2001/497/EC e 2010/87/EU in materia di SCC per il trasferimento dei dati da *controller* a *controller* e da *controller* a *processor*), la Commissione europea ha presentato due distinte bozze di decisioni volte a modificare le precedenti al fine di renderle compatibili con la sentenza medesima. Le nuove decisioni, tenuto conto che le autorità competenti di uno Stato membro possono esercitare i poteri ad esse conferiti dall'art. 28, par. 3, della direttiva 95/46/CE per sospendere o vietare a titolo definitivo i flussi di dati verso Paesi terzi ai fini della tutela delle persone per quanto riguarda il trattamento dei dati personali, richiedono agli Stati membri interessati di informare immediatamente la Commissione, la quale a sua volta deve inoltrare l'informazione agli altri Stati membri.

Al riguardo, il Gruppo Art. 29 ha reso il parere 4/2016 (WP 241, doc. web n. 6109664) con il quale, nel mostrare apprezzamento per le modifiche introdotte, oltre a proporre alcuni emendamenti alle decisioni medesime (che, in linea di massima, sono poi stati inseriti nel testo finale delle decisioni), sottolinea che le attuali modifiche apportate alle decisioni di adeguatezza non hanno comportato una rivisitazione delle decisioni in precedenza adottate per verificare che il Paese terzo di cui trattasi garantisca effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali (in particolare con riferimento alle normative e alla prassi in materia di *intelligence* e *law enforcement*), un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'ordinamento giuridico dell'Unione.

Alla luce delle considerazioni avanzate dal Gruppo Art. 29, la Commissione ha parzialmente modificato le proprie decisioni chiarendo, in particolare, che la verifica circa l'adeguatezza verrà effettuata "in fatto e in diritto".

Bcr *for controller* e Bcr *for processor*

I garanti europei continuano anche la propria attività di cooperazione nel quadro della procedura per l'adozione, a livello europeo, delle regole vincolanti d'impresa (Bcr) che possono essere utilizzate per il trasferimento dei dati effettuato tra società appartenenti ad un medesimo gruppo che operino in qualità di titolare del trattamento (Bcr *for controller*, Bcr-C) o in qualità di responsabili del trattamento

(Bcr *for processor*, Bcr-P). Nel 2016 sono state avviate 18 procedure per Bcr-C e 10 per Bcr-P e sono state concluse, con il riconoscimento dell'adeguatezza delle disposizioni nelle stesse contenute, 14 Bcr-C e 4 Bcr-P.

In 6 procedure il Garante ha fornito propri commenti in qualità *co-reviewer* al fine di rendere conformi al quadro normativo europeo i testi delle Bcr proposte dalle società (per le autorizzazioni nazionali rilasciate dal Garante, cfr. cap. 19).

24.3. *La cooperazione delle autorità nel settore libertà, giustizia e affari interni*

Europol: l'attività dell'Autorità di controllo comune (ACC)

L'ACC Europol, alla luce 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) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI, adottato l'11 aprile 2016, cesserà il proprio mandato nell'aprile 2017. La supervisione sull'attività svolta da Europol ai sensi del regolamento suddetto sarà affidata al Garante europeo per la protezione dei dati (GEPD), inclusa l'attività ispettiva, e, per assicurare una stretta cooperazione con le autorità competenti per vigilare sulla legittimità della comunicazione di dati ad Europol e garantire i diritti degli interessati, è istituito un Consiglio di cooperazione. Il Consiglio avrà funzione consultiva (cfr. art. 45 del predetto regolamento), sarà composto da un rappresentante di un'autorità di controllo nazionale di ciascuno Stato membro e dal GEPD, disporrà del supporto di un segretariato dedicato, fornito dal GEPD e di regola si riunirà almeno due volte l'anno. In vista di tale cambiamento, l'ACC Europol – che si è riunita tre volte nel corso dell'anno e che ha confermato Presidente e Vicepresidente fino ad aprile 2017 – ha proseguito la propria attività (già iniziata nel 2015, v. Relazione 2015, p. 178) volta a preparare la modifica del quadro normativo vigente, predisponendo, in particolare, un progetto di regolamento interno del Consiglio di cooperazione. Il testo è stato trasmesso formalmente, in ottobre, al GEPD con cui saranno concordati specifici incontri per pervenire ad un testo condiviso. Sono in corso inoltre contatti volti a garantire continuità al lavoro di supervisione e controllo svolto dall'ACC con incontri tematici per informare il GEPD (che sta già preparandosi ad assumere le nuove responsabilità) del lavoro svolto e mettere a disposizione dello stesso l'esperienza accumulata ed i documenti adottati che risultino ancora attuali ed utili, in particolare per quanto concerne i pareri sull'adeguatezza di Paesi terzi ed i rapporti delle ispezioni svolte.

Nel marzo 2016, si è tenuta l'ispezione annuale presso Europol che, rappresentando l'ultima svolta dall'ACC in modo dettagliato, ha avuto anche un carattere ricognitivo e di verifica delle prescrizioni contenute nei precedenti rapporti d'ispezione per valutare il grado di adempimento di queste da parte di Europol. L'Autorità ha adottato, in ottobre, il relativo rapporto prevedendo un'ulteriore ispezione nel mese di novembre per approfondire le modalità usate da Europol per raccogliere informazioni sulla rete per le finalità della lotta al terrorismo, in particolare, con l'intento di chiarire il concetto di fonti "accessibili" al pubblico ai fini della valutazione della loro liceità e correttezza. Alla luce di tale ispezione, l'ACC ha adottato uno specifico rapporto e alcune raccomandazioni. L'ACC ha inoltre deciso di svolgere nel 2017 una residua attività ispettiva limitata alla verifica dello stato di attuazione delle raccomandazioni ancora non pienamente recepite.

L'ACC ha inoltre continuato i lavori rispetto ai temi delle relazioni di Europol con i privati, alle attività da svolgere a livello nazionale per sensibilizzare le istituzioni competenti rispetto alle raccomandazioni formulate nel Rapporto sulle vittime della tratta

di esseri umani (doc. web n. 4814921) – diffuse presso le autorità competenti e rese accessibili sul sito delle DPA, e alla realizzazione della lista dei maggiori ricercati.

Il Sistema Informativo Schengen: l'attività del Gruppo di coordinamento della supervisione SIS II

Il Gruppo si è riunito due volte e ha portato a termine il lavoro avviato l'anno precedente (v. Relazione 2015, p. 179) sui modelli comuni per l'*audit* del Sistema informativo Schengen (SIS II) che potranno essere impiegati dalle DPA per le attività ispettive da svolgere in ambito nazionale. I modelli concernono l'*audit* per la sicurezza, secondo gli *standard* internazionali esistenti, e per le diverse segnalazioni che possono essere inserite nel sistema. Il Gruppo ha inoltre approvato il proprio Rapporto di attività 2013-2015 (il primo predisposto nel nuovo quadro giuridico disciplinato dal regolamento (CE) n. 1987/2006 e caratterizzato dalla nuova struttura di supervisione, operativa dal 9 aprile 2013, che include le autorità nazionali di protezione dei dati e il garante europeo per la protezione dei dati, doc. web n. 6109132) e una posizione comune (1/2016) concernente la cancellazione dal sistema delle segnalazioni relative ai veicoli ricercati a fini di sequestro o da usare come prova in procedimenti penali. Il documento contiene alcune raccomandazioni volte ad incentivare la cooperazione tra le autorità competenti dei Paesi di volta in volta interessati in modo da definire insieme le azioni da compiere, inclusa la cancellazione delle segnalazioni una volta perseguito il fine per cui le stesse erano state inserite nel sistema (doc. web n. 6109169).

Nel programma di lavoro per il periodo 2016-2018, il Gruppo ha indicato, come obiettivi per il biennio, la definizione di un quadro dei meccanismi di controllo degli accessi effettuati a livello nazionale, con la predisposizione di un questionario per le autorità nazionali responsabili della gestione del SIS II volto ad acquisire informazioni sulla politica di registrazione degli accessi allo stesso (*logging*), e un approfondimento degli aspetti legati all'applicazione dell'art. 24 del predetto regolamento (CE) n. 1987/2006 relativo alle segnalazioni degli stranieri a fini di inammissibilità.

Valutazione Schengen dell'Italia

Ha avuto luogo dal 14 al 17 marzo la terza valutazione Schengen dell'Italia relativa al settore della protezione dei dati. Il Gruppo di valutazione, formato da esperti designati delle Autorità di protezione dati di Paesi Schengen e coordinato da rappresentanti della Commissione europea, operando in base al nuovo meccanismo previsto dal regolamento (UE) 1053/2013, ha provveduto attraverso visite in loco, a verificare il grado di attuazione dato alle disposizione del regolamento e alla decisione adottati nel 2006 per disciplinare il funzionamento del sistema informativo Schengen (e del sistema informativo visti). Una parte della visita è stata dedicata al Garante, in qualità di autorità competente per la supervisione nazionale del Sistema Informativo Schengen II e di Sistema Informativo Visti (VIS), che ha illustrato la propria struttura, i poteri e le competenze, nonché le 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. Il Gruppo di valutazione ha proseguito la sua attività recandosi presso i due Ministeri che hanno illustrato le modalità di utilizzo dei due *database*. Il gruppo di valutazione al termine della visita ha predisposto un rapporto che, come da prassi, è stato sottoposto al Garante ed agli altri interessati per poter verificare l'esattezza dei riferimenti ed eventualmente presentare commenti. Il rapporto di valutazione poi, una volta discusso nei gruppi competenti di Commissione e Consiglio, sarà adottato dal Consiglio e l'Italia dovrà nei tre mesi successivi redigere il piano d'azione per porre rimedio alle eventuali mancanze rilevate.

Gruppo di supervisione Eurodac

Il Gruppo ha pubblicato, in aprile, il rapporto (doc. web n.6109073) relativo alle modalità con cui le autorità nazionali stanno dando attuazione al nuovo quadro giuridico derivante dall'adozione, il 26 giugno 2013, del regolamento (UE) n. 603/2013 (cd. Eurodac *recast*). Il rapporto contiene l'analisi delle risposte ad un

questionario fatto circolare tra le autorità nazionali competenti, il risultato dell'ispezione svoltasi il 22 settembre 2015 presso il *data center* dell'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (Agenzia EU-LISA), all'interno del quale sono ospitate le banche dati SIS, VIS e Eurodac (v. Relazione 2015, p. 179) e alcune raccomandazioni volte, tra l'altro, a richiamare l'attenzione delle autorità competenti sulla necessità di assicurare un piano per la sicurezza, procedure adeguate di cancellazione dei dati, una formazione adeguata in materia di protezione dei dati personali per il personale addetto al sistema.

Il Gruppo ha poi adottato il rapporto di attività per gli anni 2014-2015 (doc. web n. 6108706) che ha trasmesso alle istituzioni europee interessate.

Il Sistema Informativo Visti (VIS): Gruppo di coordinamento della supervisione

Il Gruppo – che si è riunito due volte nel corso dell'anno – ha adottato, a febbraio, il rapporto relativo all'accesso al Sistema Informativo Visti (VIS) e alle modalità per l'esercizio dei diritti degli interessati (doc. web n. 6109099). Il rapporto reca un quadro completo e aggiornato del funzionamento del sistema, grazie all'analisi delle risposte raccolte lo scorso anno dalle autorità nazionali sulla base di due questionari concernenti l'elenco delle autorità che a livello nazionale utilizzano il VIS, l'accesso al sistema per finalità di *law enforcement* e le modalità previste per l'esercizio dei diritti degli interessati (v. Relazione 2015, p. 180). Nel corso delle riunioni, è proseguita inoltre l'analisi delle condizioni in cui si svolge l'impiego di società private ai fini della procedura per il rilascio del visto Schengen e, sulla base di un breve questionario fatto circolare tra le autorità, è stata avviata una riflessione sulle metodologie da seguire per ispezionare il VIS e per verificare la correttezza del trattamento dei dati effettuato nell'ambito di tale sistema, anche al fine di dare attuazione all'art. 41, par. 2, del regolamento (CE) n. 767/2008 (regolamento VIS) che prevede un controllo almeno quadriennale dell'utilizzo del sistema.

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) si è riunita due volte e ha discusso del *follow-up* dell'ispezione al SID, svoltasi nel 2015, e del questionario sulla diffusione dell'opuscolo "*Guide to your responsabilities under Article 13 of the* CIS *Decision and art. 8(2)* della *Data protection framework decision*" (in italiano doc. web n. 4349259) inviato da ciascuna delegazione alle proprie autorità nazionali competenti per il sistema (v. Relazione 2015, p. 180).

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) ha adottato il rapporto di attività che copre gli anni 2014-2015 (doc. web n. 6108752) e ha proseguito la predisposizione di modelli *standard* per le ispezioni del SID. Come *follow up* del lavoro sulla guida all'esercizio del diritto di accesso adottata nel 2015 (doc. web n. 4810368), è stato anche deciso di garantirne la circolazione e l'accessibilità attraverso la pubblicazione sui siti web delle autorità di protezione dei dati e delle autorità competenti per il SID.

24.4. *Le conferenze delle autorità su scala internazionale*

La Conferenza internazionale delle autorità di protezione dati

Si è tenuta a Marrakech il 17-20 ottobre la 38ª Conferenza internazionale delle autorità di protezione dei dati. Come di consueto, la Conferenza si è articolata in una sessione chiusa per le sole autorità di protezione dei dati e una sessione aperta alla partecipazione di diversi *stakeholder*.

La sessione chiusa ha avuto inizio con l'ammissione alla Conferenza delle autorità di protezione dati di Armenia, Capo Verde, Mali e Filippine e dell'autorità delle comunicazioni della Costa d'Avorio. Sono state poi adottate le seguenti risoluzioni (disponibili al sito https://icdppc.org): a) risoluzione sulla cd. educazione digitale – di cui il Garante è stato *co-sponsor* – con la quale le autorità di protezione dei dati hanno adottato un quadro di riferimento delle competenze in materia di protezione dei dati personali per gli studenti (*International Competency Framework* che figura in allegato alla risoluzione) da divulgare tra gli operatori dell'ambito scolastico come parte della loro formazione curriculare; b) risoluzione sui nuovi parametri di misurazione delle regole di *data protection* che mira a sviluppare una metrica condivisa a livello internazionale per valutare l'impatto delle *privacy policy*; c) risoluzione sulla cooperazione internazionale in materia di *enforcement* con la quale le autorità di protezione dati sottolineano l'importanza di una effettiva e proattiva cooperazione internazionale per adempiere alle funzioni di tutela degli interessati e richiamano l'attenzione sulla necessità di sufficienti risorse umane e finanziarie per svolgere tali compiti; d) risoluzione sui difensori dei diritti umani (*human rights defenders*) che, prendendo atto dell'importanza dell'azione di associazioni e attivisti che a livello di società civile si adoperano per promuovere *privacy* e protezione dei dati, incoraggia le autorità di protezione dei dati a cooperare con le istituzioni di difesa dei diritti umani affinché tali soggetti siano supportati e protetti.

Due i *panel* tenutisi nella sessione chiusa in tema di robotica e intelligenza artificiale e di crittografia. Tra le sfide principali individuate nell'ambito di robotica e intelligenza artificiale si segnala in particolare la cd. *unpredictability by design* derivante dall'imprevedibilità dei risultati generati dai sistemi di intelligenza artificiale, nonché l'assenza di trasparenza nelle decisioni automatizzate.

In tema di crittografia, è stato discusso il difficile bilanciamento tra l'esigenza dell'industria di garantire ai propri sistemi robusti sistemi crittografici e l'accessibilità ad essi da parte delle autorità di *law enforcement*.

Tra i temi affrontati nella sessione aperta si segnalano in particolare il ruolo di *privacy* e protezione dei dati personali rispetto allo sviluppo sostenibile, il determinismo culturale e la necessità di facilitare il flusso di dati transfrontalieri senza compromettere la *privacy* e la protezione dei dati personali; il bilanciamento tra sicurezza e *privacy* e il tema della cd. *digital education*, come anticipato, rivolta non solamente a ragazzi e studenti ma anche agli educatori.

La Conferenza delle autorità europee (*Spring Conference*)

Si è tenuta a Budapest il 26 e 27 maggio la Conferenza di primavera dei garanti europei (http://www.naih.hu/budapest-springconf/).

Il segretario generale del Garante, nel suo intervento di apertura incentrato sulle novità del regolamento, in particolare il diritto alla portabilità e il rafforzamento del diritto di accesso e rettifica, ha evidenziato la necessità di rafforzare ed aggiornare il ruolo stesso della *Spring Conference*.

Nella sessione dedicata al regolamento e alle implicazioni pratiche per i legislatori nazionali, le DPA ed i titolari è stato considerato il lavoro del Gruppo Art. 29 per l'attuazione del regolamento, la necessità di una sempre maggiore cooperazione tra le autorità di protezione dati, nonché le questioni relative al delicato passaggio al nuovo quadro europeo fondato sulla condivisione di competenze tra le stesse autorità.

Una specifica sessione ha riguardato il tema della protezione dei dati da parte dei corpi di sicurezza nazionale, nella quale si è altresì discusso di Europol.

L'ultima sessione si è occupata dell'aggiornamento della Convenzione 108/1981 del Consiglio d'Europa (cfr. par. 24.5). I lavori si sono incentrati sul processo di modernizzazione della 108 e sulla necessità di raggiungere un modello di protezione

elevato, tenendo conto delle aspettative dei Paesi non appartenenti all'UE coinvolti nella elaborazione della nuova Convenzione.

Sono state adottate una risoluzione sui nuovi quadri di cooperazione e sull'importanza di una effettiva e proattiva cooperazione internazionale per adempiere alle funzioni di tutela degli interessati e una risoluzione sui flussi transfrontalieri di dati, che incoraggia le autorità di protezione dei dati a sensibilizzare gli interessati sui diritti relativi ai trasferimenti di dati e a rafforzare il loro ruolo di *enforcement* e la cooperazione internazionale in tale settore e riconosce il valore dell'accordo UE-USA sul *Privacy Shield* come migliore sistema di tutela rispetto al pregresso *Safe Harbor*.

Sono state altresì adottate le risoluzioni relative all'accreditamento alla Conferenza di: Ungheria, Gibilterra, Armenia, Cantone di Basilea-Stadt- Svizzera e Monaco.

La *Spring Conference* è stata preceduta il 25 maggio da un *workshop* del WP29 sottogruppo Cooperazione e PHAEDRA II *Project* con l'intento di approfondire il tema della cooperazione tra autorità in vista del nuovo regolamento considerando la diversità dei vari sistemi giuridici nazionali.

7ª Conferenza internazionale sulla protezione dei dati - Mosca

Si è tenuta a Mosca il 7-8 novembre la 7ª Conferenza internazionale sulla protezione dei dati organizzata dall'autorità russa (per le comunicazioni e la protezione dei dati – Roskomnadzor). La conferenza si è articolata in una sessione chiusa riservata ai delegati delle autorità per la protezione dei dati e una sessione aperta.

Durante la sessione chiusa le autorità hanno scambiato le proprie esperienze ed idee riguardo al tema dell'applicazione dei princìpi di protezione dei dati in un contesto, come quello digitale, per sua natura transfrontaliero, in particolare con riferimento all'ambito di *big data*.

La sessione aperta, alla quale hanno partecipato rappresentanti delle DPA ma anche di industria e mondo accademico, è stata dedicata a due temi principali: "*Law and education*" e "*Technology e Security*". Il segretario generale del Garante, Giuseppe Busia, ha svolto una presentazione in tema di *big data* e profilazione approfondendo le sfide e i rimedi sul piano della protezione dei dati che tali nuovi fenomeni comportano.

24.5. *La partecipazione ad altri comitati e gruppi di lavoro internazionali*

Modernizzazione della Convenzione 108 CAHDATA

Nel 2016 è stato riaperto il processo di modernizzazione della Convenzione 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

Tale revisione, cui si era dato inizio in occasione del 30° anniversario della Convenzione al fine di aggiornare il testo della 108 alla luce dei molti cambiamenti dettati dalle nuove tecnologie e dalla globalizzazione, era rimasta ferma all'adozione – avvenuta alla fine del 2014 da parte del comitato ad *hoc* del Consiglio d'Europa CAHDATA - del testo della nuova Convenzione (vedi Relazione 2014, pagg. 165 e 183 e ss.). Su tale documento pendevano tuttavia le riserve di alcune delegazioni e dell'Unione europea, allora ancora impegnata nella negoziazione del pacchetto di riforma UE sulla protezione dei dati. La modernizzazione della 108 è potuta ripartire una volta sciolti i nodi del regolamento (UE), punto necessario per poter assicurare la coerenza tra i due strumenti giuridici. Dopo l'adozione del nuovo mandato da parte del Comitato dei Ministri, il CAHDATA – di cui ha fatto parte in veste di rappresentante italiano il segretario generale del Garante - è tornato a riunirsi il 15-16 giugno 2016 per affrontare i punti irrisolti della negoziazione.

Durante la riunione, molte delle riserve dell'Unione europea sono state facilmente eliminate a fronte del fatto che il testo della Convenzione appariva in linea con il pacchetto di riforma ormai adottato a livello UE. Sono state inoltre apportate

alcune modifiche al testo della Convenzione per garantire la piena coerenza tra i due strumenti normativi (UE e CoE).

Non potendosi invece risolvere le riserve di altre delegazioni, per le quali non è stata raggiunta alcuna mediazione, il CAHDATA ha preso atto dei persistenti punti controversi demandandone la trattazione al Comitato dei ministri del Consiglio d'Europa, al quale è stata comunque trasmesso il testo della nuova Convenzione adottato dal CAHDATA seppur con le richiamate riserve.

È proseguita e si è anzi intensificata l'attività all'interno del Comitato consultivo della Convenzione 108/1981 (cd. T-PD, anche nella sua composizione ristretta, cd. T-PD Bureau) del quale il Garante – con il rinnovo del Comitato avvenuto nella plenaria del 29 giugno -1° luglio 2016 – ha assunto la presidenza.

Il T-PD, pur avendo terminato il lavoro tecnico sulla modernizzazione della Convenzione 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 CAHDATA), ha comunque continuato a seguire i lavori della revisione, in particolare esaminando il *memorandum* esplicativo che accompagnerà la nuova Convenzione e approfondendo l'attività di valutazione sulla conformità ai princìpi della 108 degli ordinamenti degli stati che sono già parti della Convenzione e di quelli che intenderanno presentare richiesta di adesione, attività che saranno entrambe di competenza del Comitato della futura Convenzione.

Il T-PD è stato inoltre impegnato nella predisposizione delle linee guida in materia di *big data*, poi adottate in procedura scritta il 23 gennaio 2017 (doc. web n. 6108739). Si tratta di una prima presa di posizione del T-PD, che, sulla base dei princìpi della 108 ma nell'ottica del testo modernizzato, si rivolge ai legislatori nazionali, ma anche ai titolari e responsabili di trattamento, evidenziando i princìpi di protezione dati cui adempiere affinché i benefici derivanti dall'impiego di *big data* possano essere perseguiti nel pieno rispetto dei diritti della persona.

Le linee guida muovono dal presupposto che la complessità e l'opacità di *big data* impongono un nuovo modo di concepire la gestione dei propri dati personali che non può essere relegata al mero controllo individuale fondato sul solo binomio informativa/consenso. Accanto ai tradizionali princìpi di protezione dati, occorre predisporre sistemi complessi di verifica preventiva dei rischi relativi all'impiego dei dati che tengano conto anche della dimensione etica del fenomeno.

È proseguito inoltre il lavoro del Comitato sulle implicazioni sulla protezione dei dati del trattamento dei *Passenger name records* (PNR) che ha portato all'adozione di uno specifico parere (19 agosto 2016, T-PD(2016)18rev, doc. web n. 6109189).

In vista della significativa interferenza con i diritti al rispetto della vita privata e della protezione dei dati rappresentati dalle misure PNR, la legalità, la proporzionalità e la necessità di tali sistemi devono essere strettamente rispettate e dimostrate in particolare attraverso: a) rappresentazioni trasparenti e misurabili della loro necessità/proporzionalità rispetto al legittimo fine perseguito; b) definizione accurata e restrittiva della legittima finalità perseguita (prevenzione, accertamento e repressione di reati terroristici o altri reati gravi o, in casi eccezionali, prevenzione di serie minacce pubbliche); c) pubblicità delle autorità competenti; d) trasmissione dei dati *push* attraverso una chiara indicazione del periodo di conservazione dei dati e appropriate misure di sicurezza; e) divieto di uso sistematico di dati sensibili; f) limitazione del *data mining* a indicatori di rischio predefiniti, con verifica –caso per caso – della rilevanza dei risultati secondo una modalità non automatizzata; g) limiti ristretti e fondati su opportuna base giuridica dei diritti dell'interessato; h) competenza delle autorità di protezione dei dati che devono essere consultate e messe nelle condizioni di verificare i sistemi PNR e di trattare ricorsi individuali; i) disponibi-

lità di rimedi amministrativi e giurisdizionali per la tutela dei diritti; supervisione esterna e indipendente del sistema PNR; f) revisione periodica dei sistemi da parte delle autorità competenti.

È proseguito altresì il lavoro di aggiornamento delle raccomandazioni sulla protezione dei dati. In particolare, come nel caso della 108, il T-PD ha lavorato su un nuovo testo della raccomandazione (97)5 sui dati sanitari, in modo da rispondere alle molte problematiche emerse nel settore a causa del sempre più frequente uso di nuove tecnologie (fascicolo sanitario elettronico, *app* mediche, RFID, ecc.). Tra le novità della raccomandazione si segnala in particolare l'introduzione della portabilità dei dati e della conseguente necessaria interoperabilità dei sistemi, nel rispetto della sicurezza dei dati e degli altri princìpi della 108.

Con riferimento alla raccomandazione (87)15 per la quale non si è ritenuto allo stato di procedere alla revisione, il Comitato ha invece optato per la predisposizione di linee guida sull'uso di dati personali in ambito di polizia che mirano a fornire indicazioni pratiche agli operatori del settore per una corretta applicazione dei princìpi della stessa raccomandazione (87)15.

Il 27 giugno 2016 è stato altresì adottato il parere sulla raccomandazione 2067 (2015) dell'Assemblea parlamentare sulla sorveglianza di massa con la quale il T-PD ha accolto con favore l'iniziativa dell'Assemblea, ha indicato nella Convenzione 108 uno strumento fondamentale, dato il suo carattere internazionale e vincolante, per la salvaguardia dei diritti rispetto a nuovi fenomeni di controllo massivo ed ha invitato il Consiglio d'Europa ad intensificare l'attività di promozione della stessa 108 al fine di favorire l'accessione anche di Paesi terzi, in particolare degli Stati che hanno già ratificato al Convenzione sul *cybercrime* (doc. web n. 6119997).

A proposito dell'adesione di nuovi Stati, il T-PD ha altresì adottato i due pareri (doc. web n. 6119997) sulla richiesta di accessione rispettivamente di Capo Verde – che ha contestualmente presentato richiesta di adesione anche alla Convenzione *cybercrime* – e della Tunisia, alla quale sono state indicate alcune modifiche necessarie per porre la normativa nazionale in piena conformità con la 108.

Il T-PD ha inoltre dato seguito positivo alla richiesta del Messico e dell'Indonesia per l'ottenimento dello status di osservatore all'interno del Comitato.

Si segnala infine l'adozione da parte del Comitato dei ministri di una nuova raccomandazione sul trattamento dei dati relativi alla salute, inclusi i dati genetici, in ambito assicurativo (2016)8, 26 ottobre 2016. La raccomandazione – sulla quale il T-PD aveva fornito parere nel 2015 sollecita i governi affinché sia assicurato il principio di non discriminazione e la protezione dei dati nell'ambito dei diversi contratti assicurativi che riguardano la vita e la salute delle persone. Tra i princìpi di protezione dati richiamati vi è il divieto di impiego dei dati genetici.

OCSE - WPSPDE

L'Autorità ha continuato a partecipare ai lavori del WPSPDE (*Working Party on Security and Privacy in Digital Economy*) dell'OCSE, anche nella sua composizione ristretta. Nel 2016 la rappresentante del Garante, già membro del Gruppo e componente del Bureau del WPSPDE, è stato riconfermata nell'incarico di vicepresidenza del Gruppo anche per il 2017.

Il primo semestre di attività è stato dedicato alla preparazione della Ministeriale OCSE 2016 che si è tenuta a Cancun (Messico) il 22-23 giugno 2016 sul tema della "Economia digitale: innovazione, crescita e sociale prosperità". Si è trattato del primo incontro Ministeriale dell'OCSE sull'economia digitale tenutosi in America Latina, riunendo ministri e oltre 1.300 partecipanti, tra cui anche rappresentanti di Paesi non membri: Argentina, Brasile, Cina, Colombia, Costa Rica, Ecuador, Egitto, Indonesia, Lettonia (che da allora è diventata il 35° membro dell'OCSE), Lituania, Malesia, Sud Africa. Preceduta da uno *stakeholder forum*, la Conferenza è stata arti-

colata in due sessioni plenarie e quattro sessioni parallele e incentrata su quattro temi, articolati ciascuno in due sessioni: Internet aperto, una piattaforma per la crescita e l'inclusione; la connettività globale; la fiducia nell'economia digitale; il lavoro e le competenze. Temi trasversali a tutte le sezioni sono stati la cosiddetta *Data Driven Innovation* (DDI), la nuova ondata di innovazione determinata dalla disponibilità di enormi volumi di dati (*big data*) e dalla capacità di estrarne conoscenza/informazione e la partecipazione delle PMI all'economia digitale (*Smes Inclusiveness*). Il nostro Paese è stato direttamente coinvolto nella preparazione dell'evento ed ha curato (tramite il lavoro del Comitato CDEP- *Committee on Digital Economy Policy* e del Gruppo WPSPDE) il percorso di discussione della "Dichiarazione ministeriale per l'economia digitale" (disponibile su https://www.oecd.org/internet/ministerial/) che i vari Ministri hanno sottoscritto al termine della Conferenza. Il WPSPDE ha in particolare organizzato il *panel* 3.2 dal titolo "*Public/Private Cooperation in Managing Digital Security and Privacy Risk for Economic and Social Prosperity*", nel quale è stato centrale il tema della protezione dati in relazione alla gestione dei rischi digitali nel contesto di "un approccio basato sul rischio" (cd. *risk based approach*, come previsto anche dal regolamento europeo). Nel corso della Conferenza è emerso come l'OCSE, attraverso il lavoro del CDEP e del WPSPDE, sia stato un antesignano nel comprendere le implicazioni e la portata che le tecnologie digitali e la protezione dei dati avrebbero avuto sull'economia e la società. La Ministeriale del 2016 ha rappresentato infatti l'approdo di un lungo percorso di analisi e di indicazioni di *policy* iniziato con la Conferenza ministeriale di Ottawa nel 1998. Da allora fino ad oggi il lavoro dell'OCSE ha avuto un ruolo decisivo nel favorire la generale comprensione di internet come una *general purpose technology* nonché nel rafforzare, tra i decisori istituzionali, la consapevolezza sulla necessità di sostenere e mantenere la sua natura aperta decentralizzata e di facilitare l'accesso alle reti ad alta velocità, approfondendo inoltre alcuni specifici ambiti di analisi quali lo sviluppo della banda larga, la sicurezza, la protezione dei dati e dei consumatori e i contenuti digitali.

Oltre al tema della Ministeriale, il WPSPDE ha portato a termine il lavoro sulla Raccomandazione sulla *governance* dei dati relativi alla salute "*Recommendation on Health Data Governance*" (disponibile su http://www.oecd.org/els/health-systems/health-data-governance.htm) adottata dal Consiglio OCSE lo scorso dicembre. Con la raccomandazione i Ministri della salute dei Paesi OCSE hanno invitato gli Stati membri ad adottare un sistema di regole comuni che consenta l'impiego e il riutilizzo dei dati sanitari per fini di pubblico interesse nel pieno rispetto della *privacy* delle persone. L'obiettivo del documento è quello di offrire indicazioni utili a migliorare e rendere più efficiente il sistema sanitario nei Paesi aderenti all'organizzazione, favorendo la creazione di una piattaforma condivisa per la corretta gestione dei dati sanitari trattati per la salute pubblica, per scopi statistici e di ricerca scientifica, nonché per la fornitura dei servizi offerti. Se ben implementate nei rispettivi Paesi, le indicazioni dell'OCSE contribuiranno anche a migliorare la qualità dell'assistenza sanitaria e, di conseguenza, a sviluppare una società "in buona salute". Tali obiettivi dovranno però essere perseguiti promuovendo e tutelando le libertà individuali e la protezione dei dati personali, peraltro a carattere sensibile, di chi usufruisce dei servizi sanitari. Nella raccomandazione vengono quindi identificati princìpi fondamentali a tutela della *privacy* che renderanno più semplice e sicura la cooperazione tra i Paesi OCSE. Tra di essi: la definizione di standard comuni per il trattamento dei dati, la necessità di informare correttamente gli utenti, il maggior coordinamento tra settore pubblico e privato, la riduzione delle barriere nello scambio delle informazioni sulla salute, assicurando al contempo l'adozione di adeguate misure a protezione delle informazioni stesse.

24

Nel 2016 il WPSPDE ha, tra l'altro, programmato e mosso i primi passi per un intenso lavoro di revisione di altre raccomandazioni OCSE ormai datate: la raccomandazione relativa alle linee guida per la crittografia (1997), la raccomandazione sulle infrastrutture critiche (2008) e la raccomandazione sulla protezione dei minori *online* (2012). Con particolare riferimento a questa ultima, ancorché meno risalente, il Gruppo ha comunque ritenuto maturo il momento del suo possibile aggiornamento, essendo profondamente mutato il contesto delle attività dei minori in rete ed i relativi pericoli (v. Relazione 2015, p. 185).

IWGDPT

L'Autorità ha proseguito la sua partecipazione all'*International Working Group on Data Protection in Telecommunication* (IWGDPT, cd. Gruppo di Berlino) che nel 2016 si è riunito a Oslo il 25-26 aprile e a Berlino il 22-23 novembre.

Il Gruppo ha lavorato sul tema dei servizi VoIP ed elaborato una bozza di documento di lavoro in materia di VoIP *security* e *privacy*. È emersa la necessità di ribadire che per i fornitori di servizi VoIP si applicano tutti gli obblighi in materia di confidenzialità delle comunicazioni, al pari di quanto avviene per i fornitori di servizi di comunicazione elettronica accessibili al pubblico. La delegazione italiana ha sottolineato le problematiche derivanti dall'ingresso di un numero assai elevato di nuovi operatori di derivazione "non statale" e talora persino stabiliti al di fuori del territorio UE, con conseguenze negative sul livello di *trust* tra le parti, la confidenzialità delle comunicazioni e l'esercizio dei diritti.

Altro tema approfondito dal Gruppo è stato quello dell'*e-learning*. Tra le questioni discusse si sottolineano: i profili di trasparenza sui dati trattati dai fornitori di servizi di *e-learning* e sulle finalità perseguite, tenendo conto che tali dati riguardano spesso minori e possono talvolta rientrare nella sfera dei dati sensibili; la presenza di soggetti terzi, rispetto ai soggetti "istituzionali" che erogano i corsi (ad es. i gestori di piattaforme) e che talora possono svolgere un ruolo di collettore "orizzontale" di dati provenienti da diversi soggetti erogatori.

In relazione all'ICANN, il Gruppo è tornato ad occuparsi del servizio WHOIS, che consente l'accesso pubblico ai dati dei *registrant* di nomi a dominio assegnati su scala globale. In particolare, il Gruppo ha espresso preoccupazioni sui trattamenti posti in essere da ICANN nella registrazioni dei nomi a dominio e in particolare sulla creazione e gestione del *database* pubblico WHOIS. Due i principali problemi: l'assenza di una finalità chiaramente dichiarata da ICANN, e il ruolo autodeterminato da parte di ICANN di vigilare sulla qualità dei dati immessi dai *registrant*. Il Gruppo ha ribadito la necessità che siano esplicitamente dichiarate le finalità perseguite da ICANN e il ruolo della catena di *registrar* che opera a livello globale, e che il tema della qualità dei dati (rilevante anche per molte istruttorie in materia di protezione dei dati personali condotte da parte delle autorità, quali i casi di *spam*) sia affrontato introducendo un sistema di accesso a due livelli: uno pubblico, che consente l'accesso al minor numero di dati, segnatamente quelli per la risoluzione di controversie tecniche, e uno dedicato alle autorità di *law enforcement* e alle autorità di protezione dati con diversi dati di contatto del *registrant* (*e-mail*, indirizzi, numeri di telefono ecc.).

Il Gruppo si è poi occupato di autenticazione biometrica (*biometric authentication*), elaborando un documento dove vengono tra l'altro precisati alcuni rischi connessi all'uso di dati biometrici, quale in particolare il *permanent tracking* dovuto alla impossibilità di revocare un dato biometrico. In proposito si è deciso di introdurre nell'*opinion* un riferimento al tema delle *revocable biometric techniques*, ossia sulle tecniche (ancora in una fase embrionale di ricerca) che rendano possibile una raccolta di dati biometrici in modo che questi possano per esempio essere cancellati in caso di incidenti.

Si segnala infine il tema delle macchine interconnesse (*connected cars*) sul quale il Gruppo ha mosso i primi passi nel 2016, ponendo attenzione all'emergente uso sempre più esteso di dati personali in questo ambito, quali i percorsi seguiti dai veicoli e, persino, le immagini relative allo stato dell'ambiente di guida interno all'autoveicolo. Le finalità di questi trattamenti sono molteplici e vanno dal controllo del traffico, allo sviluppo di piani tariffari per l'uso delle strade, fino ad azioni di *marketing* personalizzato sulle abitudini di guida. Si segnala inoltre il crescente interesse verso i dati generati dagli autoveicoli da parte dei produttori di sistemi operativi per terminali radiomobili (Android, IOS). Il Gruppo ha prodotto un primo *draft* che fa il punto dei principali rischi (mancanza di trasparenza, difficoltà nell'esercizio dei diritti) e propone alcuni rimedi.

Progetto su regolamento (UE) del CIPL (*Centre for Information Policy Leadership*)

L'Autorità ha proseguito la sua partecipazione al Progetto sul regolamento *privacy* UE organizzato dal *Centre for Information Policy Leadership (CIPL)* che nel 2016 si è riunito ad Amsterdam il 16 marzo e a Parigi il 19 settembre. Durante i due incontri, varie autorità nazionali europee di protezione dati, il Garante europeo (EDPS), i DPO (*Data Protection Officer*) dell'industria, Commissione UE e delegati dei Ministeri degli Stati membri hanno approfondito le novità introdotte dal regolamento, confrontandosi su temi cruciali per la protezione dei dati al fine di trarre delle conclusioni operative proprio laddove i diversi interessi in gioco rendono più difficile individuare soluzioni condivise.

Entrambi i *workshop* si sono rivelati utili in termini di sinergie raggiunte tra i delegati delle autorità e quelli di molte note multinazionali nella comprensione del testo del regolamento. Il Gruppo di esperti ha in particolare affrontato il tema del DPO, quale componente essenziale per la protezione dei dati del futuro quadro normativo, svolgendo un ruolo centrale all'interno delle organizzazioni. L'articolato *paper* sul DPO elaborato dal CIPL (doc. web n. 6349854) ha costituito la base della discussione sui requisiti per la nomina, la natura, la funzione e la portata del ruolo DPO alla luce delle previsioni del regolamento. Dal confronto è emerso che, mentre le nuove regole europee delineano parametri e aspettative per il ruolo del DPO, sottolineando la sua importanza in un contesto di necessaria tutela dei dati sempre più ampio, ci sono una serie di questioni che richiedono chiarimenti interpretativi (ad es. i termini "sistematico, regolare e su larga scala" relativi alla tipologia del trattamento dati che richiede la figura del DPO) per garantire un'efficace attuazione del ruolo del DPO.

Progetto CRISP

Il Garante, a seguito della partecipazione al workshop sul progetto europeo CRISP (*Evaluation and Certification Schemes for Security Products*), ha aderito alla fase finale dello stesso che prevede la stesura di un documento CWA (CEN Workshop Agreement) "*Guidelines for the evaluation of installed security systems, based on S-T-E-Fi criteria*" contenente la innovativa metodologia CRISP che considera, quali dimensioni per la valutazione di un prodotto/sistema di sicurezza, oltre alla *security* dei prodotti/sistemi, anche la fiducia degli utenti, *l'efficienza* economica e l'impatto sulle libertà e diritti individuali fra cui la protezione dei dati (*STEFi dimensions*).

Il Garante ha contribuito in particolare alla revisione della *checklist* allegata al documento contenente domande e requisiti per la valutazione delle diverse dimensioni.

Cooperazione internazionale IECWG, GPEN, PHAEDRA *project*

Nel 2016 è proseguita l'attività dei Gruppi di lavoro dedicati al coordinamento delle attività internazionali di *enforcement*, come richiesto dalla 37ª Conferenza internazionale delle autorità di protezione dati e dal lavoro del Gruppo di coordinamento delle attività internazionali di *enforcement* – IECWG (v. Relazione 2015, p. 184-185).

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 2016 ha dedicato il *Privacy Sweep* (indagine a carattere internazionale) alla verifica del rispetto della *privacy* nell'Internet delle Cose - IoT (*Internet of Things*). Il Garante, membro del GPEN, ha partecipato attivamente allo *Sweep* sugli IoT, prendendo in esame dispositivi molto diversi: dai contatori intelligenti ai termostati regolabili via web, dalle *smart-cars* agli orologi intelligenti che misurano il battito cardiaco e la pressione sanguigna, dal controllo a distanza degli ascensori ai frigoriferi che segnalano la scadenza dei cibi. Il Garante ha concentrato la sua azione in particolare sulla domotica per verificare il grado di trasparenza nell'uso delle informazioni personali dei consumatori e il rispetto delle norme sulla protezione di dati da parte delle aziende, anche multinazionali, operanti nel settore. Oltre a quella italiana, altre ventotto autorità garanti della *privacy* di altrettanti Paesi del mondo hanno preso parte all'indagine. Dall'analisi su oltre trecento dispositivi elettronici connessi a internet portata avanti dalle predette autorità è emerso un quadro globale poco confortante: più del 60% non ha superato l'esame dei Garanti dei diversi Paesi.

Incontri con le delegazioni estere e organizzazioni internazionali

L'Autorità ha continuato a partecipare a programmi di partenariato europeo negli ambiti di competenza, offrendo la propria esperienza per facilitare l'avvicinamento delle normative dei Paesi coinvolti al quadro comunitario in materia di protezione dei dati.

In tale contesto, il Garante e l'autorità statale per la protezione dei dati personali della Repubblica del Kosovo hanno sottoscritto un impegno di reciproca assistenza in materia di protezione dei dati personali, al fine di promuovere il rispetto dei diritti umani e delle libertà fondamentali e di sviluppare iniziative mirate di cooperazione anche di lungo termine. L'accordo, siglato nel mese di maggio a Budapest, nell'ambito della Conferenza di primavera delle autorità europee per la *privacy* (vedi *supra*), si inserisce nel quadro della cooperazione già attivata dal Garante italiano con altre autorità dell'Est europeo, come Romania, Albania, Macedonia. L'Agenzia statale per la protezione dei dati personali della Repubblica del Kosovo e il Garante svilupperanno iniziative comuni di interesse per entrambe le istituzioni e avvieranno una costante attività consultiva bilaterale.

Parimenti, nel mese di settembre 2016 il Garante ha ricevuto presso la propria sede una delegazione dell'Autorità per la protezione dei dati moldava nel corso della quale l'Autorità italiana e quella moldava hanno sottoscritto un impegno di reciproca assistenza in materia di protezione dei dati personali, volto a promuovere il rispetto dei diritti umani e delle libertà fondamentali ed a consentire attività di cooperazione anche di lungo termine. Anche tale accordo si inserisce nel quadro della cooperazione attivata dal Garante italiano con altre autorità dell'est europeo, prevedendo tra i vari punti, lo scambio di esperti, la condivisione delle informazioni e delle migliori pratiche, anche al fine di individuare soluzioni armonizzate tra i due Paesi.

Il 18 ottobre presso il Garante si è tenuto un incontro con una delegazione del programma di *Technical Assistance* della Banca Mondiale/IFC (WBG – *World Bank Group*), relativo al *credit reporting* per le regioni MENA (Middle East and North Africa) e Africa Sub Sahariana. Durante l'incontro l'Ufficio ha svolto presentazioni sulle competenze e le principali attività del Garante, sulle più importanti decisioni dell'autorità in ambito bancario e finanziario, con particolare riferimento al codice di condotta dei sistemi informativi creditizi, e sulle sanzioni.

25 L'attività di comunicazione, informazione e di rapporto con il pubblico

25.1. *La comunicazione del Garante: profili generali*

L'attività di informazione e comunicazione del Garante è stata caratterizzata nel 2016 da una sempre più decisa azione di sensibilizzazione nei confronti di cittadini, imprese, pp.aa. sul ruolo cruciale che assume la protezione dei dati nel mondo digitale. Da una parte l'inarrestabile sviluppo delle tecnologie di raccolta e analisi dei dati personali presenti in rete e le enormi potenzialità che esse offrono in campo sociale, scientifico, economico; dall'altra i rischi di una profilazione sempre più sofisticata e invasiva, nonché di una crescente concentrazione di ingenti quantità di informazioni nelle mani di pochi colossi del web, determinano sempre più forti esigenze di assicurare idonee garanzie a tutela della *privacy* attraverso un bilanciamento tra diritti ed interessi in tensione, ivi compreso quello tra esigenze di sicurezza e rischi di sorveglianza indiscriminata e generalizzata degli individui.

Centrale è stato l'impegno di informazione e comunicazione teso ad illustrare le novità introdotte, in termini di garanzie per le persone e di obblighi per la p.a. e le imprese, dal regolamento europeo sulla protezione dei dati personali – che è entrato in vigore nel maggio 2016 e sarà direttamente applicabile in tutti gli Stati membri dell'Unione dal 25 maggio 2018.

Un altro tema sul quale l'Autorità si è particolarmente impegnata è stato quello della vulnerabilità delle grandi banche dati e della messa in guardia contro i rischi del *cybercrime*. Il Garante ha più volte richiamato l'attenzione sulla necessità di porre tra gli *asset* strategici la messa in sicurezza dei dati archiviati e il patrimonio informativo di imprese e pp.aa..

Il Servizio relazioni esterne e *media* del Garante ha da tempo progressivamente attuato e raffinato un programma di comunicazione istituzionale utilizzando diversi canali divulgativi sui molteplici settori di interesse dell'Autorità quali il *cyberbullismo* e la scuola, le informazioni commerciali, la sanità, la tutela dei minori specie nel mondo dell'informazione, il diritto all'oblio, il controllo dei lavoratori, il recupero crediti, il *telemarketing,* lo *spam*, il fisco e la trasparenza *online* nella p.a..

Ulteriori temi di particolare rilevanza sociale sono stati quelli legati all'uso delle biometrie sul posto di lavoro, il registro dei tumori, i diritti dei consumatori, la reputazione *online*, la sicurezza dei cittadini, la fecondazione assistita, l'anagrafe degli studenti, i nuovi accordi internazionali tra Europa e USA in tema di *privacy*, i *fake* sui *social network*, l'*e-commerce*, la sicurezza delle grandi banche dati, i *data breach*, i *big data* e l'Internet delle Cose (IoT).

Con riguardo a quest'ultimo profilo, si evidenzia la partecipazione del Garante all'"indagine a tappeto" (*sweep*), di carattere internazionale, avviata dalle autorità per la protezione dei dati personali appartenenti al *Global Privacy Enforcement Network* (GPEN), allo scopo di verificare il rispetto della *privacy* nelle numerose e diversificate fattispecie inquadrabili nell'Internet delle Cose. I riscontri raccolti dagli esperti delle autorità, su più di trecento *app* delle principali società del settore, hanno fatto emergere, a livello globale, gravi carenze nella tutela della *privacy* degli utenti: il 59% delle *app* non offre informazioni adeguate sulle modalità di raccolta, di utilizzazione e comunicazione dei dati personali; il 68% non fornisce appropriate informazioni

sulle modalità di conservazione dei dati; il 72% non spiega agli utenti come cancellare i dati dal dispositivo; il 38% non garantisce semplici modalità di contatto ai clienti che desiderano chiarimenti in merito al rispetto della propria *privacy*. Dall'analisi di alcuni dispositivi sono emerse criticità anche sulla sicurezza dei dati (ad es., la trasmissione in chiaro, quindi in modalità non criptata, al medico curante di informazioni relative alla salute degli utenti).

Sotto il profilo del contrasto al fenomeno del bullismo e della violenza in rete, nonché della promozione di un uso corretto e consapevole del web e dei *social network* il Garante ha continuato, inoltre, a dare il proprio contributo nell'ambito dell'*Advisory Board* istituito nell'ambito del *Safer internet center* presso il Miur.

I *media* hanno mantenuto una costante attenzione sulle problematiche riguardanti la tutela dei dati personali e sull'attività del Garante. Nel 2016 il Servizio relazioni esterne e *media* ha selezionato circa 52.000 articoli di interesse per l'Autorità. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali, delle testate *online* e *blog* che hanno trattato i temi legati alla *privacy* sono state 14.350 delle quali 4.060 dedicate esclusivamente all'attività del Garante. Le prime pagine sono state 984, di cui 279 riguardanti la sola Autorità. Le interviste, gli interventi e le dichiarazioni del Presidente e dei Componenti pubblicate sulla carta stampata sono state complessivamente 205, mentre 223 quelle *online* e 43 quelle andate in onda su tv e radio nazionali e locali. Le citazioni relative al tema della *privacy* e all'attività del Garante in programmi televisivi e radiofonici nazionali sono state oltre 250.

25.2. *I prodotti informativi*

Nel 2016 sono stati diffusi 37 comunicati stampa e 13 *newsletter*. La *newsletter* del Garante è una pubblicazione periodica – giunta al suo XVIII anno di diffusione (per un totale di 423 numeri e di 1.453 notizie) – che consente un ampio approfondimento rispetto ai più importanti provvedimenti adottati dall'Autorità nei diversi settori di intervento, alla sua attività in ambito europeo ed internazionale e alle molteplici iniziative legate alla diffusione della cultura della protezione dei dati personali. Le notizie pubblicate vengono redatte a cura del Servizio relazioni esterne e *media*, composte graficamente e completate con l'aggiunta di immagini per la versione web. La *newsletter* – la cui lista di distribuzione è costituita da oltre 8.000 destinatari – viene inviata via *e-mail* a redazioni, professionisti, pp.aa., imprese e singoli cittadini che ne fanno richiesta. Allo scopo di favorire una più ampia utilizzazione di questo importante strumento di informazione, sul sito del Garante è attiva la possibilità di iscriversi *online* alla *newsletter*. È poi possibile consultare l'archivio tematico della *newsletter* che raccoglie gli articoli prodotti in 18 anni. Anche l'archivio storico dei comunicati stampa è consultabile sul sito istituzionale.

25.3. *I prodotti editoriali e multimediali*

Il Garante per promuovere la propria attività, semplificare la comprensione dei principali provvedimenti adottati e favorire la cultura della protezione dei dati personali, utilizza diversi strumenti che si differenziano per tipologia e *target* di utenza.

Nell'ambito della Collana editoriale del Garante, "Contributi", è stato pubblicato il volume "La società sorvegliata. I nuovi confini della libertà", per il quale il Servizio ha curato l'*editing* dei testi e il progetto grafico e che raccoglie le relazioni

di studiosi ed esperti intervenuti al convegno organizzato dall'Autorità in occasione della Giornata europea della protezione dei dati personali 2016 (doc. web n. 5312018). L'Autorità ha poi curato la pubblicazione, nell'ambito dei *vademecum*, di una nuova guida concernente "La *privacy* a scuola" (doc. web n. 5602011) che dedica particolare attenzione alla scuola 2.0 e al corretto uso delle nuove forme di comunicazione e condivisione in internet, al fine di prevenire atti di *cyberbullismo* e di "riaffermare quotidianamente, anche in ambito scolastico, quei princìpi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino" (cfr. dichiarazione del presidente Soro, doc. web n. 5601934).

L'opuscolo raccoglie i casi affrontati dal Garante con maggiore frequenza ed offre elementi di riflessione e indicazioni per i tanti quesiti posti al riguardo dalle famiglie e dalle Istituzioni: da come trattare correttamente i dati personali degli studenti (in particolare quelli sensibili, come condizioni di salute o convinzioni religiose) a quali regole seguire per pubblicare dati sul sito della scuola o per comunicarli alle famiglie; da come usare correttamente *tablet* e *smartphone* nelle aule scolastiche a quali cautele adottare per i dati degli allievi con disturbi di apprendimento. Per facilitarne la consultazione, la guida è articolata in cinque brevi capitoli (Regole generali; Vita dello studente; Mondo connesso e nuove tecnologie; Pubblicazione *online*; Videosorveglianza e altri casi) e in due sezioni "di servizio" (Parole chiave; Appendice - per approfondire) utili per comprendere meglio la terminologia utilizzata dal legislatore e per avere un sintetico quadro giuridico di riferimento. Il *vademecum* è stato distribuito in formato elettronico a circa 56.000 scuole statali e a 13.000 scuole paritarie, nonché in formato cartaceo a diversi istituti scolastici.

Oltre alla realizzazione di prodotti editoriali è stata elaborata nel tempo una significativa serie di prodotti multimediali diffusi anche mediante canali *social*, grazie ai profili istituzionali aperti dal Garante su Linkedin, YouTube e Google+. Anche nel periodo di riferimento non sono mancati nuovi prodotti multimediali messi a disposizione degli utenti sul sito istituzionale del Garante: video, guide, *vademecum* digitali, schede infografiche – pensati non soltanto per utenti esperti quali, ad es. i nativi digitali. Tutti i prodotti multimediali sono realizzati esclusivamente dal personale del Servizio relazioni esterne e *media* del Garante, che ne cura tutte le fasi della creazione (scrittura e adattamento testi, progetto grafico, impaginazione, sceneggiatura, sviluppo animazione e selezione/costruzione degli elementi visivi, scelta delle musiche e sincronizzazione, registrazione dei testi, adattamento audio, montaggio e *post*-produzione).

Come accennato nel paragrafo precedente, a seguito dell'entrata in vigore del regolamento (UE) in materia di protezione dei dati personali e in vista della sua definitiva applicazione, il Garante si è impegnato in iniziative tese a sensibilizzare e informare le persone e ad accompagnare le pp.aa. e le imprese nella fase di prima applicazione del regolamento.

L'Autorità ha infatti predisposto sul suo sito web istituzionale una sezione dedicata al regolamento (UE) (http://www.garanteprivacy.it/regolamentoue) che sarà costantemente arricchita con informazioni e documenti di interesse. In particolare, sono stati resi disponibili: una prima guida sintetica al regolamento (disponibile anche in formato di infografica, doc. web n. 5187635); una pagina informativa (www.garanteprivacy.it/rpd) sul Responsabile della protezione dei dati - Rpd (*Data Protection Officer* - DPO), che contiene anche un'infografica sull'innovativa figura (doc. web n. 4791352); una pagina tematica dedicata al cd. pacchetto protezione dati (http://www.garanteprivacy.it/pacchettoprotezionedati), ovvero l'insieme della normativa europea in materia di *privacy* che, oltre al regolamento, comprende anche

la direttiva sui trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini.

La menzionata guida digitale al "Nuovo regolamento europeo in materia di protezione dei dati personali" contiene semplici e sintetiche informazioni su alcune tra le principali innovazioni previste dal nuovo regolamento (UE): il diritto all'oblio e quello alla portabilità dei dati; la nuova figura del Responsabile della protezione dei dati; l'obbligo di comunicare le violazioni e gli attacchi informatici subiti; i limiti alla profilazione delle persone sono alcuni degli aspetti trattati nell'opuscolo (doc. web n. 5187723).

L'Autorità ha, inoltre, predisposto il *vademecum* digitale "*Privacy* e recupero crediti. Le regole per il corretto trattamento dei dati personali" (doc. web n. 4893274), una guida sintetica che illustra in modo semplice ed immediato i princìpi a cui si devono ispirare coloro che svolgono attività di recupero del credito e le garanzie riconosciute al debitore.

Lo strumento delle infografiche, che raccoglie un significativo riscontro da parte degli utenti, ha inaugurato un nuovo filone comunicativo che utilizza un *format* compatto (una singola pagina), una schematizzazione che risponde contemporaneamente ad esigenze di sintesi e completezza, e una grafica accattivante che facilita la presentazione immediata dei contenuti più significativi di iniziative e provvedimenti. Tali strumenti si prestano particolarmente alle esigenze di diffusione e veicolazione dei messaggi attraverso il web e, in particolare, i *social media*.

Nel 2016 sono state predisposte un'infografica (doc. web n. 5295490) e una pagina informativa (doc. web n. 5306161) dedicate al *Privacy Shield.* I documenti illustrano in modo sintetico ed efficace gli elementi principali del nuovo accordo fra Unione europea e Stati Uniti d'America che impone alle imprese americane obblighi più stringenti in materia di protezione dei dati personali degli europei, in linea con la decisione della CGUE, che aveva invalidato il precedente accordo detto *Safe Harbor*. Il *Privacy Shield* prevede in particolare che le autorità americane assicurino con più forza il rispetto dell'accordo e collaborino con le Autorità europee per la protezione dei dati. L'accordo contiene – per la prima volta – dichiarazioni e impegni assunti formalmente in merito all'accesso ai dati da parte di varie figure istituzionali dell'Amministrazione americana.

È stata inoltre elaborata la scheda infografica intitolata "Violazioni di dati personali (*data breach*): gli adempimenti previsti" quale strumento informativo di facile ed immediata consultazione sui vari provvedimenti riguardanti i differenti settori per i quali sono previste comunicazioni da parte dei titolari in caso di *data breach* (doc. web n. 5033588).

Anche sul codice delle informazioni commerciali è stata ideata e realizzata un'infografica (doc. web n. 5268223) che illustra in sintesi le regole più rilevanti fissate dal nuovo codice di deontologia (doc. web n. 4298343), entrato in vigore a ottobre 2016 e rivolto alle società che raccolgono e offrono informazioni sull'affidabilità commerciale di imprenditori e *manager* (cfr. par. 15.2). Anche in questo caso, l'infografica ha consentito di riassumere, come un mini *vademecum*, gli elementi salienti del documento, evidenziando gli aspetti più rilevanti e rendendo più agile la consultazione del testo.

Ad una delle tecniche illecite più diffuse, utilizzate per appropriarsi delle informazioni riservate delle persone è dedicata l'infografica intitolata "*Phishing*: attenzione ai "pescatori" di dati personali" (doc. web n. 5779928) la quale, in modo semplice e chiaro, illustra il fenomeno e fornisce consigli utili per evitare che malintenzionati si impossessino dei nostri dati personali. Con questo prodotto, il Garante ha inteso avviare un approfondimento sul tema della cd. *Cybersecurity*, oggetto di

importanti preoccupazioni da parte degli operatori di molteplici settori, nonché dei privati cittadini, soprattutto in ragione della gravità dei danni informatici già verificatesi e di quelli potenziali.

Sono state create o potenziate diverse pagine informative del sito web, costantemente aggiornate. In particolare, va ricordata l'apertura di un *repository* che classifica per area tematica i pareri del Garante (doc. web n. 5469251) che verrà progressivamente arricchito e aggiornato, e che al momento comprende tre sezioni di approfondimento sui temi dello Spid – Sistema pubblico d'identità digitale (doc. web n. 5657277), della Banca dati dna (doc. web n. 5468580) e dell'Ampliamento dati nella dichiarazione precompilata 2017 (doc. web n. 5469399).

Per quanto riguarda le iniziative istituzionali sui *social media* attivate dal Garante, si registra una costante crescita di interesse non solo da parte di un'utenza generalista (che segue soprattutto il profilo Google+, https://plus.google.com/u/1/+GarantedatipersonaliGP), ma anche di quella più specialistica (in particolare professionisti dell'area giuridica e informatica) che utilizza il profilo LinkedIn dell'Autorità (https://www.linkedin.com/company/autorit-garante-per-la-protezione-dei-dati-personali). In particolare, l'incremento dei *followers* registrato nel 2016 è pari al 31% raggiugendo quota 6.000. Una speciale attenzione è stata poi dedicata all'implementazione del profilo Google+, sfruttando le potenzialità comunicative del *social media*: in particolare, si è provveduto alla creazione di varie *repository* tematiche che offrono agli utenti aggiornamenti semplici e puntuali su svariate tematiche di interesse.

Sempre sul fronte *social media*, si è investito sulla viralizzazione dei contenuti informativi attraverso la creazione di *badge* grafici che consentono di riproporre con modalità innovative contenuti di interesse specifico. Una particolare attenzione è stata dedicata – in collaborazione al lavoro del Responsabile trasparenza e anticorruzione – all'adeguamento della sezione Autorità trasparente (http://www.garanteprivacy.it/web/guest/home/trasparenza) in relazione alle nuove disposizioni normative previste in materia (cfr. par. 26.3).

25.4. *Le manifestazioni e le conferenze*

Giornata europea della protezione dei dati

Il 28 gennaio di ogni anno, a partire dal 2007, viene celebrata la Giornata europea della protezione dei dati personali, un'iniziativa promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte le Autorità preposte alla protezione dei dati personali nei Paesi europei. In tale giorno, scelto per ricordare in tutta Europa l'adozione della convenzione di Strasburgo n. 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato dei dati da parte di governi, parlamenti, organi per la protezione dei dati personali e altri soggetti, vengono svolte attività e iniziative dirette ad accrescere la consapevolezza sui diritti legati alla tutela della vita privata e delle libertà fondamentali. Tali attività comprendono campagne mirate per gli utenti, progetti didattici per gli istituti scolastici, incontri organizzati presso le autorità per la protezione dei dati. In questo quadro, nel 2016 il Garante ha organizzato il convegno dal titolo "La società sorvegliata. I nuovi confini della libertà", che si è svolto a Roma, nell'aula del Palazzo dei gruppi parlamentari. Quanto controllo può sopportare una democrazia? Quali sono gli aspetti più problematici della raccolta indiscriminata e massiva di dati personali da parte di agenzie governative e colossi del web? Quali rischi comporta il ricorso a strumenti di controllo sempre più invasivi? Quale impatto sta avendo non solo sull'economia e sull'organizzazione sociale, ma anche sulla nostra vita privata l'uso dei

25

big data? *Privacy* e sicurezza sono davvero in contrasto quando si tratta di combattere il terrorismo e la criminalità informatica? Sono queste alcune delle questioni oggetto di analisi e riflessione del convegno i cui lavori sono stati aperti e chiusi dal Presidente Soro. Nella prima sessione, "Quanto controllo può sopportare una democrazia?", sono intervenuti Marco Minniti, sottosegretario alla Presidenza del Consiglio dei ministri, il sociologo Giuseppe Roma e il magistrato Armando Spataro. A coordinare il dibattito Augusta Iannini, vicepresidente dell'Autorità. Nella seconda sessione, che ha trattato il tema "Condivisione, profilazione, *big data*" sono intervenuti il giornalista Fabio Chiusi, il filosofo Maurizio Ferraris e l'avvocato Guido Scorza, coordinati da Giovanna Bianchi Clerici, componente del Garante. E nella terza sessione, coordinata da Licia Califano, anch'essa componente del Garante, è stato approfondito il tema "*Privacy* e sicurezza nella società digitale" con le relazioni dell'avvocato Gian Domenico Caiazza, della giornalista Stefania Maurizi e del magistrato Carlo Nordio.

Nel suo discorso di apertura, il presidente Soro ha sostenuto che la "Libertà [è] sempre più insidiata da forme di controllo sottili, pervasive e capaci per questo di annullare – se non adeguatamente regolate – ogni possibilità per l'individuo di «costruirsi liberamente»". "Sono convinto – ha affermato il Presidente dell'Autorità – che dovremmo contrastare la deriva per cui la persona è considerata come una «miniera a cielo aperto» da cui attingere liberamente, per elaborare profili – individuali, familiari, di gruppo – funzionali ai bisogni di una società compressa tra le esigenze di sicurezza, incalzata dagli interessi dei produttori di tecnologie, minacciata da sottili strategie di esclusione. É anche per questo che la *privacy* come libertà dal controllo è condizione della democrazia e del pluralismo, presupposto di dignità e garanzia contro ogni discriminazione". Anche quest'anno, con l'obiettivo di coinvolgere le giovani generazioni su temi di tale portata e valenza civica, al convegno sono stati invitati, tra gli altri, gli studenti di due licei romani.

Altri convegni

Il 29 aprile a Cagliari, il presidente Soro ha partecipato alla tavola rotonda: "*Privacy*, trasparenza e anticorruzione: quale equilibrio?" concludendo i lavori con un suo intervento dal titolo "La parabola della trasparenza". " […] binomio trasparenza e *privacy* rappresenta un tema di grande rilievo nel nostro tempo: un tempo di crisi non solo economica, ma dei modelli politici, dell'idea stessa di cittadinanza, degli stessi legami sociali", ha sottolineato il Presidente. "L'estensione progressiva delle misure di trasparenza e l'avvicendarsi così rapido delle modifiche legislative – secondo il Presidente dell'Autorità – se da un lato hanno contribuito a rafforzare gli strumenti di sindacato diffuso in chiave partecipativa, hanno dall'altro privato, in molti aspetti, la disciplina della necessaria ragionevolezza e coerenza".

Nel 2016 il Garante ha anche partecipato ai convegni organizzati da Google nell'ambito della campagna informativa "Vivi internet, al sicuro" che ha avuto come obiettivo quello di fornire ai cittadini italiani, giovani e non, gli strumenti per un uso consapevole del web. La menzionata campagna informativa prevedeva una serie di incontri di riflessione e confronto su temi di interesse quali: la *cybersecurity*, il regolamento (UE) 2016/679, il rispetto della *privacy* nelle imprese, le *start up*, la tutela dei consumatori e dei minori. Gli incontri, a molti dei quali hanno partecipato i vertici del Garante, si sono svolti presso alcune Università (Roma Tre, Bocconi, Alma Mater Studiorum, Federico II, Salerno e Cagliari). Il 7 novembre, all'Università degli Studi di Napoli Federico II, il presidente Soro ha introdotto il tema su "La tutela dei minori nel mondo digitale"; la vicepresidente del Garante, Augusta Iannini, è intervenuta agli incontri del 10 ottobre a Roma e del 14 novembre a Bologna per parlare del "Il nuovo regolamento sulla protezione dei dati personali e il *Privacy Shield* UE-Usa: nuove regole e sfide per lo sviluppo", e dell'

"Economia digitale e commercio elettronico: sicurezza, *privacy* e fiducia"; all'Università Bocconi, il 17 ottobre la componente dell'Autorità Giovanna Bianchi Clerici ha partecipato al convegno dedicato a "Il ruolo degli operatori pubblici e privati tra libertà di espressione e sicurezza di internet"; all'Università di Cagliari il 24 ottobre, il segretario generale, Giuseppe Busia, ha parlato di "*Start-up* e la protezione dei consumatori in internet".

Per il decimo anno consecutivo Consumers' Forum ha organizzato l'incontro, tenutosi a Roma il 17 novembre, con le maggiori Autorità indipendenti italiane ed intitolato "Authority e Consumatori. Dalla *sharing* alla *social economy*". In tale sede il Presidente ha avuto l'opportunità di ribadire che "Il tema dell'economia digitale, in tutte le sue articolazioni coinvolge sempre di più le autorità indipendenti che oggi possono esercitare forme di regolazione più agili per governare i processi di rapido cambiamento indotto prodotti dalle innovazioni tecnologiche. Mai come oggi appare evidente come la protezione dei dati rappresenti una risposta all'avanzare di una tecnologia incontrollata e il presupposto essenziale per garantire un giusto equilibrio tra innovazione e tutela delle garanzie dei cittadini".

Nell'ambito del convegno organizzato da Crif "Referenza creditizia ed innovazione: benefici per il consumatore e nuove sfide per i regolatori" (Roma, 14 novembre) è intervenuto il presidente Soro che ha anche illustrato l'importanza del codice deontologico – sottoscritto da tutte le associazioni rappresentative del settore creditizio oltre che da quelle dei consumatori – che disciplina, in modo organico, l'attività svolta dalle "centrali rischi" private. Tale codice è rivolto principalmente alla tutela del consumatore contro il rischio di un improprio uso delle informazioni che lo riguardano raccolte nei sistemi di informazioni creditizie (Sic). "Importante è, infatti" – ha sottolineato Soro – la qualità delle informazioni trattate per la valutazione del merito creditizio. Una informazione non corretta, non aggiornata può avere ricadute gravi sul cittadino e addirittura privarlo della possibilità di accedere al credito".

La 4ª edizione del festival della scienza e dell'innovazione si è svolta a Settimo Torinese dal 15 al 23 ottobre. Nell'ambito di tale manifestazione il presidente Soro ha partecipato all'incontro "Noi più liberi dei robot?" nel corso del quale è stato presentato anche il libro scritto dallo stesso Presidente "Liberi e connessi", pubblicato nella primavera del 2016 da Codice edizioni.

25.5. *Le relazioni con il pubblico*

Assistenza al pubblico e predisposizione di nuovi strumenti informativi

A conferma del *trend* degli anni precedenti, anche nel 2016 l'attività dell'Ufficio relazioni con il pubblico – che consiste prevalentemente nella consulenza ai visitatori in sede e per telefono, nonché nella gestione delle moltissime richieste pervenute via *e-mail* – è stata molto intensa (cfr. sez. IV, tab. 15 e 16) ed ha riguardato tematiche e criticità in materia di protezione dei dati personali, con una particolare attenzione all'esercizio del diritto d'accesso e degli altri diritti riconosciuti alle persone fisiche dal Codice, soprattutto nell'ambito dei trattamenti svolti sul web e del cd. diritto all'oblio.

Nel fornire assistenza a cittadini, enti e imprese, l'Ufficio ha sempre coniugato approfondimento giuridico, cortesia e tempestività nella risposta, caratteristiche che gli sono valse attestazioni di stima e apprezzamento da parte dell'utenza.

La particolare funzione svolta dall'Urp, primo e diretto interlocutore del Garante verso l'esterno, gli ha consentito anche quest'anno di individuare con tempismo novità ed "emergenze" di particolare rilevanza sociale o economica, meritevoli di

25

essere sottoposte al vaglio dell'Autorità, anche mediante lo strumento della reportistica interna sulle tematiche di maggiore evidenza predisposta a vantaggio delle altre unità organizzative.

Al fine di migliorare l'offerta informativa del Garante in aggiunta alle modalità più tradizionali di informazione, anche nel 2016 l'Urp ha poi curato la predisposizione di FAQ in collaborazione con il Dipartimento o Servizio interessato, in particolare in materia sanitaria e, precisamente, riguardanti referti *online* (doc. web n. 5734352), *dossier* sanitario (doc. web n. 5806006) e Fascicolo sanitario elettronico (doc. web n. 5805978) presenti sul sito dell'Autorità.

Gli oltre 23.500 contatti gestiti dall'Ufficio (16.000 circa dei quali via *e-mail*), confermano anche per il 2016 l'alto livello di attenzione dell'opinione pubblica nei confronti della tutela dei dati personali e dell'attività del Garante. Oltre a ciò, si segnalano 444 affari definiti e 268 visitatori ricevuti presso la sede dell'Ufficio.

Tematiche d'interesse

Come già rilevato nelle precedenti Relazioni, anche nel 2016 sono state sottoposte all'Urp molteplici questioni afferenti alla normativa in materia di protezione dei dati personali, tra queste si evidenzia ancora, per la rilevanza nel dibattito istituzionale e per la molteplicità di segnalazioni ricevute, il *marketing* selvaggio e, in particolare, effettuato con il telefono. Il fenomeno è ancora causa di grande disturbo per i cittadini, come confermano anche le oltre 5.100 *e-mail* ricevute, molte delle quali riguardano le cd. chiamate mute. In concomitanza con la scadenza dei termini previsti per alcuni adempimenti hanno poi suscitato particolare interesse (e sono state quindi oggetto di numerose richieste di chiarimento) le nuove previsioni normative concernenti la localizzazione di *call center* in Paesi *extra*-UE contenute nell'art. 24-*bis,* d.l. 22 giugno 2012, n. 83 (convertito, con modificazioni, dalla l. 7 agosto 2012, n. 34) come modificato dalla l. 11 dicembre 2016, n. 232.

Sempre oggetto di attenzione è poi la questione del *marketing* via sms, fax e *e-mail*, rispetto alla quale le segnalazioni ricevute sono state oltre 1.100. Anche la questione delle attivazioni di servizi a pagamento non richiesti sulle utenze di telefonia mobile effettuate nel corso della navigazione in internet – sulla quale il Garante ha da tempo in corso complessi accertamenti presso i diversi soggetti a vario titolo coinvolti nel fenomeno – è stata più volta segnalata all'Ufficio. Sempre in ambito Tlc, si segnalano le richieste degli utenti relative all'accesso ai dati di traffico telefonico e telematico e, in particolare, ai dati concernenti le chiamate in entrata, disciplinate, come noto, con particolare cautela dal Codice.

Un gran numero di richieste ha avuto ad oggetto la nuova normativa introdotta dal regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati), che, come già più volte detto, è entrato ufficialmente in vigore il 24 maggio 2016 e diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018. Al riguardo, moltissime sono state le richieste relative alla nomina, alle responsabilità e al ruolo del Responsabile della protezione dei dati personali, in particolare nel rapporto con le altre figure previste dalla normativa.

Un altro tema al centro di numerose istanze è quello concernente i trattamenti di dati personali effettuati da soggetti pubblici per finalità di pubblicità e trasparenza sul web (d.lgs. n. 33/2013). Si registrano numerose richieste provenienti da enti pubblici, oltre che da cittadini interessati, soprattutto a seguito delle modifiche apportate al d.lgs. n. 33/2013 dal d.lgs. 25 maggio 2016, n. 97.

Anche la videosorveglianza, con riferimento all'ambito condominiale, lavorativo e scolastico, è stata oggetto di numerosi quesiti e richieste (oltre 1.000 *e-mail*) relative, in particolare, alla possibilità di utilizzare le videocamere nelle case di cura e negli asili nido, nonché all'uso delle cd. *dashcam*, ossia sistemi di videoripresa montati, per scopi diversi, a bordo di veicoli. Sempre molto alto il numero delle richie-

ste concernenti l'installazione, ad opera di privati, di impianti di videosorveglianza in ambito condominiale.

Anche nel 2016 hanno suscitato grande interesse le questioni concernenti i trattamenti di dati personali nell'ambito dei *social network* e del web in generale (oltre 1.000 *e-mail*), soprattutto a seguito della tragica vicenda di una giovane donna, le cui immagini erano state diffuse in rete contro la sua volontà. I problemi riguardano non solo le vittime di casi analoghi, ma anche coloro che abbiano inizialmente deciso di condividere *online*, attraverso *social network* o servizi di messaggistica, i propri dati e vogliano successivamente eliminarli o, quanto meno, evitare che vengano indicizzati dai motori di ricerca. In tale contesto si inseriscono anche le istanze relative ai trattamenti in ambito giornalistico e alla gestione dei cd. archivi storici *online* dei quotidiani, ove sempre delicata è l'azione di bilanciamento degli opposti interessi in gioco (diritto alla riservatezza, da un lato, e interesse pubblico della notizia, dall'altro).

Molti sono stati i quesiti concernenti i trattamenti di dati personali effettuati in ambito sanitario, con particolare riferimento alle previsioni relative alla ricetta dematerializzata, al *dossier* sanitario e al Fse, questi ultimi non a caso oggetto delle menzionate FAQ.

Oltre 660 *e-mail* hanno riguardato, poi, i trattamenti in ambito lavorativo. Si segnalano, in particolare, oltre alle questioni legate all'utilizzo delle telecamere negli ambienti di lavoro, i temi connessi all'uso di internet e della posta elettronica sul posto di lavoro, al trattamento di dati sensibili correlato al riconoscimento di permessi o benefici, al controllo a distanza dei lavoratori mediante geolocalizzazione, al rilevamento delle presenze dei lavoratori mediante sistemi tecnologicamente avanzati, *in primis* mediante l'uso di dati biometrici.

A conferma della sempre crescente consapevolezza degli utenti circa l'importanza e la trasversalità del diritto alla protezione dei dati personali, rispetto ai dati dello scorso anno risultano notevolmente aumentate le richieste relative agli adempimenti e agli strumenti di tutela previsti dal Codice (oltre 1.800 *e-mail*) riguardanti una molteplicità di settori, in alcuni casi pervengono ancora da persone giuridiche che però come noto, non possono più ricorrere ai predetti strumenti (segnalazioni, reclami e ricorsi) riservati dal 2011 alle sole persone fisiche (d.l. 6 dicembre 2011, n. 201, cd. decreto salva-Italia, convertito con l. 22 dicembre 2011, n. 244).

Anche le questioni concernenti i trattamenti di dati nell'ambito dei sistemi di informazioni creditizie e l'accesso ai dati bancari sono state oggetto di moltissimi quesiti e segnalazioni (in totale oltre 1.200 *e-mail*), come pure numerose sono state le richieste relative al codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale (provv. 17 settembre 2015, n. 479, doc. web n. 4298343). Al riguardo, sono state in particolare evidenziate le tematiche riguardanti il trattamento dei dati personali dei soci, dei sindaci e in generale dei soggetti che rivestono cariche societarie, le modalità e i tempi di conservazione delle informazioni trattate, la comunicazione e la diffusione delle informazioni provenienti da fonti pubbliche.

Sempre numerose, infine, le richieste di chiarimenti, pervenute soprattutto da consulenti e imprese, aventi ad oggetto le clausole contrattuali *standard*, le Bcr (*Binding corporate rules)* e il cd. *Privacy Shield*, l'accordo adottato il 12 luglio 2016 dalla Commissione europea che regolamenta il trasferimento di dati tra Unione europea e USA.

26 Studi, documentazione, trasparenza e anticorruzione

26.1. *Il Servizio studi e documentazione*

Predisposizione della Relazione annuale

Il Servizio studi ha coordinato la predisposizione del testo della Relazione annuale sull'attività svolta nel 2015 e sullo stato di attuazione del Codice. Essa costituisce un importante adempimento normativo ed istituzionale previsto dall'art. 154, comma 1, lett. *m*), del Codice il quale, nell'individuare i compiti dell'Autorità, menziona anche la rappresentazione dell'attività svolta nell'anno solare di riferimento al Parlamento e al Governo.

Nel 2014 il legislatore aveva inoltre introdotto l'obbligo per le autorità amministrative indipendenti, tra le quali il Garante, di dare conto nella Relazione annuale del rispetto delle disposizioni concernenti la razionalizzazione delle autorità medesime e di trasmettere la Relazione in parola anche alla Corte dei conti (art. 22, d.l. n. 90/2014 convertito in l. 11 agosto 2014, n. 114).

In questo quadro la Relazione persegue un'effettiva finalità di trasparenza sull'attività svolta dall'Autorità non soltanto rispetto ai soggetti destinatari per legge della Relazione ovvero Parlamento, Governo e Corte dei conti, ma anche nei confronti della collettività, tenuto conto che essa viene pubblicata e resa disponibile sul sito istituzionale del Garante.

La Relazione costituisce inoltre un prezioso strumento di conoscenza per diverse categorie di utenti interessati, a vario titolo, alla materia della protezione dei dati. Essa è infatti costituita da una parte generale ed introduttiva sui principali interventi effettuati dall'Autorità e da molteplici sezioni tematiche (ivi comprese quelle di natura statistica) idonee a fornire, in modo rapido e sintetico, informazioni puntuali sull'attività svolta nel periodo di riferimento (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.

Infine la redazione della Relazione rappresenta tradizionalmente un'importante occasione di riflessione e analisi interna anche ai fini della programmazione dell'attività e dei possibili miglioramenti nell'esercizio del ruolo di garanzia dell'Autorità.

Attività di documentazione

Analogamente agli anni passati, il Servizio ha svolto attività di documentazione interna funzionale all'aggiornamento del personale attraverso la redazione periodica di un notiziario interno denominato "Osservatorio *privacy*" recante una rassegna di normativa, giurisprudenza, dottrina e documentazione proveniente da soggetti pubblici e privati nazionale comunitaria ed internazionale in materia di protezione dati e su questioni di interesse per l'Autorità. Al riguardo, a titolo meramente esemplificativo, si menzionano tra le questioni segnalate nell'Osservatorio *privacy* quelle del diritto del figlio a conoscere le proprie origini dopo la morte della madre biologica in caso di parto anonimo (Corte di cassazione nn. 22838 e 15024/2016), dello scudo UE-USA per la *privacy* a seguito della sentenza della CGUE (6 ottobre 2015 causa C-362/14, Maximillian Schrems/Data Protection Commissioner) nonché quella delle intercettazioni di conversazioni o comunicazioni tra presenti, eseguite mediante l'installazione di un "captatore informatico" (Corte di cassazione sez. unite penali n. 26889/2016).

Il Servizio ha inoltre fornito, a mezzo di atti interni, elementi di valutazione ai fini della formulazione dei pareri richiesti dalla Presidenza del Consiglio dei ministri per l'eventuale impugnazione davanti alla Corte costituzionale delle leggi regionali ritenute di dubbia conformità limitatamente alla materia della protezione dei dati personali (cfr. par. 3.4) e in altri casi, come ad esempio, in relazione ai pareri resi dall'Autorità ai sensi dell'art. 154, comma 4, del Codice (cfr. par. 3.3.1).

26.2. *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 – ulteriormente valorizzata dal completamento della catalogazione in OPAC e dalla sua immissione in internet – è nata per supportare le attività di informazione, di ricerca e di studio dell'Autorità; i servizi all'utenza esterna sono pertanto complementari (anche in ragione delle risorse disponibili) rispetto a questo fine istituzionale. Nel contesto generale di prosecuzione della razionalizzazione della spesa e di predisposizione delle operazioni di trasloco nella nuova sede, dotata anche di spaziosi magazzini, l'Ufficio ha avviato il trasferimento dell'intero patrimonio direttamente accessibile nonché delle collezioni precedentemente custodite in magazzini, allo scopo di riunificare l'intero posseduto bibliografico e di riallestire successivamente una o più sale di lettura e di consultazione (cfr. par. 27.2).

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 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 istituzioni bibliotecarie. In termini di comparazione con il patrimonio bibliografico della biblioteca dell'Autorità e per l'utilità dei riscontri statistici (aggiornati al 31 dicembre 2016), il sistema SBN cataloga con il vocabolo "*privacy*" nel titolo 1.325 documenti a stampa (1.176 monografie, +107 sul 2015, 694 delle quali in italiano); 180 monografie con la stringa di "protezione dei dati" nel titolo (+ 19 sul 2015); 191 monografie con l'espressione di *"data protection"* (+ 22 sul 2015); 78 monografie con il vocabolo "*Datenschutz"* nel titolo (+ 4 sul 2015); 431 monografie (365 in

italiano) sotto il soggetto di "Diritto alla riservatezza" (rispettivamente + 87 e + 92 sul 2015). Il Polo Bibliotecario Parlamentare cataloga sotto il soggetto "riservatezza (diritto)" 1.103 *records* (503 in italiano) (rispettivamente + 121 e + 8 sul 2015). I *records* aventi il vocabolo *"privacy"* nel titolo sono 360 (213 in italiano, 120 alla Camera e 93 al Senato); quelli aventi nel titolo la stringa "protezione dei dati" sono 129; quelli con l'espressione di "*data protection*" 59; quelli con il vocabolo "*Datenschutz*" 46.

Nel 2016 i servizi all'utenza interna ed esterna hanno funzionato in modo ridotto fino al mese di luglio e nel secondo semestre sono stati sospesi a causa del nuovo trasloco. Questi i dati relativi agli utenti interni: 543 i documenti richiesti in lettura; 105 i prestiti; 335 le richieste di fotoriproduzioni; 42 i casi di assistenza bibliotecaria (34 *online*); 8 le riproduzioni di documenti con inoltro in formato elettronico. Questi i dati sul pubblico esterno: 7 le autorizzazioni alla frequentazione; 74 i titoli consegnati in lettura; 136 le richieste di fotoriproduzioni; 222 i casi di assistenza bibliografica *online*; 43 gli invii di *Document Delivery*. La consultazione del catalogo OPAC sulla intranet ha registrato 3.424 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 2016 ha superato il traguardo di ca. 150.000 operazioni (cifra ottenuta sommando il numero di ricerche e quello delle visualizzazioni), con un incremento del 50% rispetto al 2015, anno che aveva già fatto registrare il *record* di oltre 100.000 operazioni. Il *database* con il più elevato conteggio ha registrato 7.516 sessioni di lavoro (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 89.103 documenti consultati (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. 34 connessioni e 405 documenti (30 connessioni e 326 documenti nel 2015, 30 connessioni e 364 documenti nel 2014, 28 connessioni e 337 documenti nel 2013).

26.3. *L'Autorità trasparente e l'anticorruzione*

Nel 2016 la normativa in materia di prevenzione della corruzione e della trasparenza è stata innovata ed integrata per effetto dell'entrata in vigore del d.lgs. 25 maggio 2016, n. 97 (revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche) (cfr. par. 2.1.2).

Al riguardo, nel fare rinvio al par. 4.3. in merito all'attività svolta dall'Autorità sui profili di interesse della normativa in parola, giova ricordare che il Garante, sin dal 1998 ha progressivamente introdotto nel proprio ordinamento misure di prevenzione della corruzione, fra l'altro adottando un analitico codice etico (delibera 4 giugno 1998) e attuando la normativa in materia di obblighi di pubblicazione e di trasparenza di cui al d.lgs. n. 33/2013.

Il Garante, con delibera del 12 ottobre 2016, n. 414 (doc. web n. 5568742), ha ritenuto opportuno dare attuazione "agli adempimenti previsti dalla normativa sulla prevenzione e repressione della corruzione e dell'illegalità", e, in particolare, provvedere alla nomina del "Responsabile della prevenzione della corruzione, nonché all'adozione di un proprio piano triennale per la prevenzione della corruzione".

Con la menzionata delibera il Garante ha quindi nominato per la prima volta il Responsabile della prevenzione della corruzione e della trasparenza (RPCT) il cui nominativo è stato pubblicato nella sezione "Autorità trasparente" del sito istituzionale e comunicato all'Anac. L'Autorità ha, in tal modo, unificato in capo allo stesso dirigente l'incarico di Responsabile della prevenzione della corruzione e quello di Responsabile della trasparenza il quale ha espletato la propria attività tenendo conto di quanto stabilito con delibera 15 dicembre 2016, n. 522 (doc. web n. 5802906) in merito agli obiettivi strategici in materia di prevenzione della corruzione e trasparenza. In questo ambito, il RPCT ha provveduto a effettuare l'attività preparatoria e di studio con particolare riguardo alla predisposizione del Piano triennale di prevenzione della corruzione e della trasparenza 2017-2019 adottato dal Garante nel mese di gennaio 2017.

È stata, poi, avviata l'attività di formazione del personale in materia di prevenzione della corruzione e trasparenza provvedendo, quale prima fase, per il periodo restante del 2016, alla primaria ed indispensabile formazione del RPCT e del personale di supporto.

Con specifico riguardo alla trasparenza, l'Autorità ha prestato prioritaria attenzione all'adeguamento alle innovazioni introdotte dal d.lgs. n. 97/2016, proseguendo l'attività di impulso e monitoraggio sull'adempimento degli obblighi normativamente previsti nonché l'aggiornamento della sezione "Autorità trasparente" del sito web istituzionale anche con riguardo alla modifica della disciplina in materia di accesso civico, parimenti introdotta dal d.lgs. n. 97/2016.

A questo titolo sono pervenute le prime richieste di accesso civico, delle quali alcune presentate in sede di riesame e altre hanno riguardato la pubblicazione obbligatoria dei dati (nessuna delle quali, peraltro, ha dato luogo ad un adeguamento perché i dati risultavano già pubblicati).

Alla tematica della prevenzione della corruzione e della trasparenza e, in particolare, del corretto contemperamento delle misure volte ad attuare la trasparenza amministrativa con i diritti fondamentali delle persone, con specifico riferimento alla riservatezza e al diritto alla protezione dei dati personali è stato dedicato l'intervento del presidente Soro al convegno tenutosi a Cagliari il 29 aprile 2016 su "*Privacy*, trasparenza e anticorruzione: quale equilibrio?" (cfr. par. 25.4).

L'Ufficio del Garante

III - L'Ufficio del Garante

27 La gestione amministrativa e dei sistemi informatici

27.1. *Il bilancio e la gestione economico-finanziaria*

La gestione amministrativa dell'Autorità, già improntata ai princìpi generali della contabilità finanziaria, economica e patrimoniale, è stata caratterizzata da significative modifiche volte ad adeguare le procedure alle esigenze di armonizzazione dei sistemi contabili e degli schemi di bilancio delle amministrazioni pubbliche previste dalle vigenti disposizioni.

Con l'adozione del bilancio di previsione 2016, infatti, si è provveduto ad articolare la rappresentazione della spesa anche per missioni e programmi e si è dato corso all'implementazione del piano dei conti integrato, previsto per la generalità delle amministrazioni in regime di contabilità finanziaria. Attraverso tali adeguamenti è stato assicurato un miglioramento della qualità delle informazioni ed una maggiore trasparenza dei dati contabili, riconducibile ad un sistema univoco di rilevazione delle entrate e delle spese, secondo comuni criteri di contabilizzazione.

Il bilancio dell'Autorità è stato improntato al rispetto del princìpio della prudente valutazione delle entrate ed all'attenta programmazione delle spese, nell'osservanza delle procedure e dei vincoli di spesa contenuti nelle disposizioni legislative e regolamentari applicabili anche al Garante.

Una particolare attenzione è stata rivolta nell'assicurare che le scelte gestionali – orientate all'esclusivo perseguimento delle finalità istituzionali ed all'adempimento degli obblighi dettati dalle disposizioni nazionali e dell'Unione europea – fossero improntate al pieno rispetto dalle vigenti norme in materia di *spending review* e ad una generalizzata realizzazione di economie di spesa.

Riguardo alle specifiche esigenze di contenimento degli oneri di gestione, l'Autorità ha posto in essere tutti gli adempimenti per gestire i propri servizi logistici con criteri di economicità, nel rispetto delle prescrizioni di cui all'art. 22, comma 9, d.l. 24 giugno 2014, n. 90, convertito, con modificazioni, dalla l. 11 agosto 2014, n. 114.

Un primo obbligo scaturente da tale disposizione prevede, tra i criteri che devono essere rispettati per la gestione dei propri servizi logistici, l'ubicazione della sede in un edificio di proprietà pubblica.

In tale ottica, quindi, nel 2016 – al fine di dismettere i locali sede degli uffici del Garante, di proprietà privata – sono stati perfezionati gli atti per la stipula di un nuovo contratto di locazione in un edificio di proprietà pubblica. Il trasloco delle singole unità organizzative del Garante, già avviato alla fine dell'anno, dovrà completarsi nel corso dell'esercizio 2017.

Come per il passato, l'Autorità non detiene immobili adibiti ad abitazione o foresteria.

27

Si dà atto, infine, che nell'anno di riferimento la spesa per incarichi di consulenza è stata limitata ad un singolo intervento, resosi necessario per garantire la sicurezza ed il corretto funzionamento delle procedure di notificazione telematica dei trattamenti, ed il relativo importo è risultato comunque largamente al di sotto dei limiti di spesa consentiti dalle vigenti disposizioni legislative.

La gestione amministrativa del Garante, oltre ad essere assoggettata agli ordinari e periodici controlli dell'organo preposto alla verifica della regolarità amministrativo-contabile, è stata sottoposta ad una puntuale attività di indagine e di verifica da parte della Corte dei conti con un procedimento che, iniziato nel corso del 2015, si è concluso con l'adozione della deliberazione 12 maggio 2016, n. 2/2016/G (doc. web n. 5799684) cui ha fatto seguito una nota del Presidente del Garante in cui sono state indicate tutte le misure che l'Autorità ha inteso adottare, nonché le motivazioni sottese alle scelte da effettuare o effettuate a seguito dei rilievi formulati (nota 13 giugno 2016, doc. web n. 5511913).

Sotto il profilo più strettamente contabile, il risultato dell'esercizio ha fatto registrare un lieve avanzo di amministrazione, pari a 0,8 milioni di euro, che evidenzia una gestione in sostanziale equilibrio finanziario. Nel 2016, infatti, le entrate complessivamente acquisite dall'Autorità sono state pari a 19,9 milioni di euro a fronte delle quali sono stati registrati impegni di spesa per 19,1 milioni di euro.

Le risorse finanziarie acquisite al bilancio del Garante sono rappresentate, per la parte più significativa, da trasferimenti assicurati da altre autorità amministrative indipendenti, per un totale di 10,0 milioni di euro.

È opportuno evidenziare che la specifica disposizione legislativa, in base alla quale è stato disposto il trasferimento delle risorse finanziarie in questione, ha esaurito i propri effetti con l'esercizio 2016. Va dato atto, tuttavia, che il Parlamento, nell'ambito della disciplina degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea, con la l. 7 luglio 2016, n. 122 ha disposto una rimodulazione dei trasferimenti in favore del Garante per la protezione dei dati personali, i cui oneri dal 2017 graveranno esclusivamente sui fondi erariali, assicurando in tal modo una migliore razionalizzazione del sistema di finanziamento della stessa Autorità ed una continuità gestionale.

Gli stanziamenti erariali registrati nel corso dell'anno sono risultati complessivamente pari a 9,3 milioni di euro, dei quali 6,6 milioni di euro a titolo di contributo ordinario per il funzionamento posto a carico del bilancio dello Stato, nella misura prevista dalla legge di stabilità, e 2,7 milioni di euro a titolo di anticipazioni per riassegnazione delle sanzioni comminate dal Garante. Le ulteriori e marginali entrate (0,6 milioni di euro) sono ascrivibili ad entrate proprie per diritti di segreteria e proventi residuali di diversa natura.

Dalla tabella 19 (cfr. sez. IV) si evince che, rispetto al corrispondente valore del precedente esercizio finanziario, nonostante una lieve flessione del contributo ordinario gravante sul bilancio dello Stato (in valore assoluto –0,2 mil. di euro, pari a –3,77%), l'importo delle entrate complessivamente accertate fa registrare un incremento del 3,37% (in valore assoluto 0,6 mil. di euro). Tali somme sono state utilizzate per lo svolgimento delle attività istituzionali e dei compiti assegnati dalla legge e dalle disposizioni regolamentari europee.

La spesa complessiva fa registrare un incremento poco significativo rispetto al precedente esercizio (in valore assoluto 0,4 mil. di euro, pari al 2,04%), la cui variazione denota uno scostamento essenzialmente fisiologico tra le due annualità a raffronto.

La struttura della spesa è caratterizzata, come per la generalità di analoghi soggetti pubblici, da una significativa incidenza degli oneri per il personale, la cui com-

ponente, tuttavia, rappresenta per esperienza, competenza e professionalità un fattore di primaria importanza nell'espletamento delle molteplici funzioni cui l'Autorità è chiamata ad adempiere, sia in ambito nazionale, sia attraverso una costante partecipazione nelle pertinenti sedi istituzionali europee.

Le indennità di carica dei componenti del Garante non hanno subito variazioni ed il loro importo è comunque contenuto entro i prescritti limiti di legge.

Con riferimento, infine, agli oneri strettamente connessi alle esigenze gestionali, nel corso dell'anno risultano rispettati, tra l'altro, i limiti riguardanti la spesa complessiva per consumi intermedi prevista dalle specifiche disposizioni di cui al d.l. 6 luglio 2012, n. 95, convertito, con modificazioni, dalla l. 7 agosto 2012, n. 135 e successive integrazioni.

Anche riguardo alle spese di mobilità e per l'esercizio di autoveicoli, le vigenti disposizioni di limitazione della spesa risultano pienamente adempiute. In tale ottica, infatti, l'Autorità si avvale per le complessive esigenze di mobilità sul territorio comunale di un unico autoveicolo, assegnato in comodato d'uso dalla competente autorità governativa.

27.2. *L'attività contrattuale, la logistica e la manutenzione dell'immobile*

Attività contrattuale

Nel 2016 l'attività contrattuale dell'Autorità si è svolta, come di consueto, in attuazione degli obiettivi generali del Garante e in conformità alla vigente normativa, con particolare riferimento all'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), secondo il quale 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".

Si sono infatti concluse nell'anno in questione due procedure gestite in comune con altre autorità che hanno sottoscritto apposita convenzione attuativa della richiamata disposizione di legge: una Richiesta di Offerta sul Mercato elettronico della p.a. avviata in comune con l'Autorità per l'energia elettrica il gas e il sistema idrico per la fornitura di cancelleria e una gara comune con l'Autorità di regolazione dei trasporti avente ad oggetto l'affidamento del servizio di *brokeraggio* assicurativo. Grazie alle citate procedure sono stati conseguiti significativi risparmi sui lotti di competenza, rispetto alla base di gara (70% per la cancelleria e 40% circa per il *broker*).

Nel contempo, sono proseguiti i lavori finalizzati alla gestione unitaria dei servizi strumentali ed in particolare sulla possibilità di svolgere in comune le procedure per i servizi di copertura assicurativa per l'Autorità (sanitaria, r.c.t.o, *all risks* mobiliare, immobiliare, elettronica, vita e invalidità permanente).

Durante il periodo in considerazione sono stati ampiamente utilizzati gli strumenti messi a disposizione da Consip sul portale Acquistinretepa.it e, oltre alle convenzioni, sono stati realizzati numerosi acquisti a mezzo Richiesta di Offerta (RdO) e Ordini Diretti d'Acquisto (ODA) sul MePA, nei termini previsti dalla normativa.

Relativamente alle convenzioni Consip, oltre a quelle ad adesione obbligatoria *ex* d.l. n. 95/2012 (energia elettrica, servizio sostitutivo di mensa mediante buoni pasto, carburanti tramite *fuel card*), l'Ufficio ha altresì aderito alla convenzione relativa alla gestione integrata della sicurezza sui luoghi di lavoro, individuando le necessità relative alla corretta applicazione del d.lgs. n. 81/2008. Mediante ricorso alla procedura di RdO sul MePA sono stati acquisiti i servizi di trasloco della sede

dell'Autorità, di cui si dirà in seguito, nonché il servizio di progettazione grafica e comunicazione visiva, con un ribasso relativo medio di oltre il 25%. Per quest'ultima procedura, l'istruttoria ha avuto impulso dalla necessità di individuare un operatore economico in grado di soddisfare, nel breve e medio termine, le complesse esigenze di progettazione grafica dell'Autorità, che impegnavano, per ogni singolo affidamento, le risorse di più di un ufficio. Gli affidamenti sono stati gestiti, a partire dall'anno di riferimento, sotto forma di accordo-quadro, con un importante semplificazione della procedura interna di acquisizione del servizio.

Appare opportuno evidenziare – in presenza delle categorie merceologiche di riferimento – la priorità con la quale l'Autorità ha fatto ricorso agli strumenti Consip e alle procedure comparative anche per importi inferiori a 40.000 euro e che gli affidamenti diretti effettuati al di fuori del MePA sono stati inferiori al 10% del totale degli acquisti, con un importo medio estremamente contenuto, pari a circa 1.250,00 euro cadauno.

Con riguardo poi 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 gli strumenti di acquisto e negoziazione del portale Consip.

Sono state effettuate solo 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, oppure a causa della mancata attivazione di nuove convenzioni da parte di Consip, nei tempi previsti; tale ultima fattispecie ha riguardato, in particolare, il contratto di *facility management* per la sede dell'Autorità, il cui contratto stipulato in adesione alla previgente convenzione Consip è scaduto in data 31 dicembre 2016.

Un significativo impegno di risorse è stato destinato alla gestione della delicata fase di prima attuazione del d.lgs. n. 50/2016 (codice dei contratti pubblici), a decorrere da aprile 2016, anche alla luce delle linee guida Anac pubblicate nel corso dell'anno; sono state altresì avviate, con gli Uffici dell'Autorità, le attività finalizzate alla definizione della programmazione biennale degli acquisti, come previsto dal nuovo codice.

Sotto altro profilo, le modifiche intervenute relativamente agli obblighi di trasparenza previsti dal d.lgs. n. 33/2013 hanno comportato la revisione delle attività, anche relativamente al profilo della normativa anticorruzione.

Nel periodo considerato è stata effettuata l'attività istruttoria concernente un'indagine della Corte dei conti, a seguito della quale l'Ufficio ha elaborato un documento analitico, corredato – con particolare riferimento al numero e agli importi degli affidamenti – da elementi di dettaglio, riguardante specificamente l'attività negoziale del Garante.

Logistica e manutenzione dell'immobile

Con riferimento alla logistica e manutenzione dell'immobile l'attività è stata particolarmente intensa, anche a seguito del recesso dal contratto di locazione effettuato dalla società proprietaria dell'immobile dove ha sede l'Autorità, con la relativa necessità di un'accelerazione delle procedure finalizzate alla individuazione di una nuova sede, peraltro già avviate da tempo. Infatti l'Autorità, in vista della scadenza del contratto di locazione nel 2017, aveva già esperito da circa due anni una significativa attività di ricerca per un immobile da adibire a propria sede, interessando prioritariamente amministrazioni ed enti pubblici, come previsto dal d.l. n. 90/2014. Nel periodo in esame sono quindi proseguite le interlocuzioni con i soggetti pubblici – *in primis* l'Agenzia del demanio – per il reperimento di una nuova sede, ed è stata altresì effettuata una ricerca di mercato presso gli operatori privati, che non ha però dato esiti soddisfacenti. Le predette attività hanno infine condotto

all'individuazione di una nuova sede, di proprietà pubblica, presso l'immobile denominato Palazzo Wedekind, sito in piazza Colonna – Roma, offerto in locazione dalla Società IGEI S.p.A. in liquidazione, cui è affidata la gestione del patrimonio immobiliare dell'Inps.

Tutte le attività riguardanti il trasloco della sede, compresa la procedura comparativa riguardante l'individuazione dell'operatore del servizio di trasloco, sono state avviate nel 2016, e se ne ipotizza la conclusione nel secondo semestre 2017, non risultando tuttora pienamente disponibili le aree di destinazione.

Infine è proseguita l'ordinaria operatività di logistica e manutenzione dell'immobile a supporto agli interventi previsti dal citato contratto di *facility management*, in adesione alla convenzione Consip.

27.3. *L'organizzazione dell'Ufficio*

Nel 2016, oltre all'istruttoria sull'indagine della Corte dei conti concernente la gestione amministrativa e finanziaria relativa al periodo 2012-2015 (art. 3, comma 4, l. n. 20/1994) di cui si è detto nel par. 28.1, è proseguita la rigorosa attuazione delle disposizioni previste dal d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122. In tale quadro, in relazione ad un intervento tecnico di estrema urgenza, nel periodo considerato è stato conferito un solo incarico di consulenza di brevissima durata.

Con riguardo alla convenzione quadro in materia di procedure concorsuali per il reclutamento del personale delle autorità indipendenti – siglata nel 2015 ai sensi dell'art. 22, comma 4, d.l. n. 90/2014, al fine di disciplinare le procedure da seguire nel caso in cui un'autorità intenda bandire un concorso e le regole per la gestione congiunta delle procedure allorché una o più autorità manifestino interesse alla copertura delle figure professionali oggetto del bando – nel 2016 sono state bandite da altre autorità alcune procedure concorsuali alle quali il Garante, in ragione della specificità dei profili richiesti, non ha ritenuto di aderire, procedendo all'istruttoria necessaria per il ricorso a procedure di mobilità volontaria esterna per funzionari, da espletare nel 2017.

Tenuto conto dei precedenti protocolli d'intesa sottoscritti nel 2002 e 2005, e dell'eccellente livello di collaborazione tra le due Istituzioni, è stato rinnovato il protocollo d'intesa con la Guardia di finanza al fine di consentire al Garante di disporre di personale con specifica competenza e pregressa esperienza in attività di polizia giudiziaria e polizia amministrativa. Nel corso dell'anno, inoltre, è stato siglato un importante accordo con Equitalia S.p.A. in base al quale, in un'ottica di collaborazione tra amministrazioni e di scambio di competenze e di esperienze di interesse specifico, il Garante si è impegnato ad ospitare per un anno due funzionari appartenenti ai ruoli della predetta Società.

Con riferimento alle misure di sicurezza previste dal d.lgs. n. 81/2008 in materia di sicurezza sui luoghi di lavoro, l'Ufficio – in seguito all'adesione alla convenzione stipulata tra Consip e il RTI composto da EXITone S.p.A. (Capogruppo) e Studio Alfa S.r.l., per l'affidamento dei servizi relativi alla gestione integrata della salute e sicurezza sui luoghi di lavoro – ha provveduto a strutturare tutta la complessa attività e gli innumerevoli adempimenti, provvedendo ad organizzare tutti i corsi previsti dalla normativa.

Servizio di Segreteria del Collegio

Nel corso dell'anno il Servizio di Segreteria del Collegio ha seguito lo svolgimento delle attività dell'organo collegiale e, in particolare, la predisposizione e la distribuzione della documentazione necessaria per le adunanze, la conservazione dei

verbali delle riunioni e degli originali delle deliberazioni adottate nonché del materiale utile per la pubblicazione in Gazzetta Ufficiale.

Conformemente a quanto disposto dall'art.15 del Regolamento n.1/2000 e nel rispetto del Cad, la Segreteria del Collegio 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. Il Servizio ha garantito il controllo dei provvedimenti collegiali prima dell'invio alla redazione web per la pubblicazione sul sito istituzionale dell'Autorità ed ha peraltro contribuito a provvedere sulle richieste di oscuramento dei dati personali pervenute dagli interessati o dai titolari del trattamento, a vario titolo, coinvolti, in particolare con riferimento a esigenze di riservatezza riguardo a casi di segreto industriale o *know out* tecnologico.

27.4. *Il personale e i collaboratori esterni*

Nel 2016 sono stati collocati in posizione di fuori ruolo presso il Garante due militari della Guardia di finanza e distaccati, per un periodo di un anno, due funzionari di Equitalia S.p.A (cfr. par. 27.3).

Nello stesso periodo sono stati rinnovati tre contratti a tempo determinato per il personale di diretta collaborazione assegnato all'organo di indirizzo politico.

Analogamente agli altri anni sono state espletate due procedure, ciascuna delle quali funzionali alla selezione di 5 giovani laureati per l'effettuazione di periodi di tirocinio presso l'Autorità. Nel corso dell'anno, 10 giovani laureati hanno quindi svolto un periodo di formazione e orientamento presso il Garante.

Al 31 dicembre 2016 l'Ufficio poteva contare su una dotazione organica, a diverso titolo, di 137 unità, di cui 113 in servizio, al quale va aggiunto un contingente di personale a contratto di 8 unità (cfr. sez. IV, tab. 17 e 18). Dai suddetti dati si evidenzia che nell'anno considerato si è verificato un incremento di n. 3 unità di personale in servizio, rispetto all'anno precedente. Particolare attenzione è stata riservata, anche nel 2016, all'attività formativa per il personale.

In particolare, la convenzione stipulata con la Scuola nazionale dell'amministrazione ha consentito la partecipazione gratuita di un elevato numero di dipendenti ai corsi di formazione da questa organizzati. È stato svolto, inoltre, un corso formativo interno di aggiornamento, sugli applicativi più comunemente usati per una migliore gestione dei documenti informatici, seguito con molto interesse da un rilevante numero di dipendenti.

L'Autorità, inoltre, in seguito ad una procedura comparativa effettuata sul MePA, ha erogato 5 corsi di formazione di lingua inglese (due di livello avanzato e tre di livello intermedio).

Complessivamente, nel corso dell'anno sono state somministrate circa 243 ore di formazione, che hanno interessato circa il 70% del personale.

Anche nel periodo considerato, l'Autorità si è avvalsa delle figure professionali previste dalla vigente normativa in materia di sicurezza e incolumità dei lavoratori nei luoghi di lavoro (medico competente e responsabile del servizio di prevenzione e sicurezza), i cui contratti, tuttavia, sono stati prorogati solo per il tempo necessario a verificare le condizioni della convenzione Consip concernente l'affidamento dei servizi relativi alla gestione degli adempimenti previsti dal citato d.lgs. n. 81/2008, alla quale l'Autorità ha aderito con decorrenza 1° luglio 2016.

Presso l'Autorità, infine, opera il servizio di controllo interno che è presieduto da un magistrato della Corte dei conti e composto da due dirigenti generali, rispettiva-

mente, della Ragioneria generale dello Stato e della Presidenza del Consiglio dei ministri.

27.5. *Il settore informatico e tecnologico*

Sviluppo del sistema informativo e dei servizi ICT

Nel 2016 è proseguita l'attività di sviluppo del sistema informativo con l'implementazione del sistema di gestione documentale delle adunanze collegiali avviato nel corso del 2015 e in costante evoluzione in ragione della pressante richiesta di nuove e ulteriori funzionalità a sostegno dell'efficienza dell'attività amministrativa.

Dal punto di vista infrastrutturale, è stata completata l'azione di consolidamento delle architetture a supporto delle applicazioni del sistema informativo, che si basa su un'infrastruttura virtuale che consente di operare con più elevati livelli di *fault-tolerance* ed è predisposta per l'integrazione con servizi di *cloud computing*.

È stato inoltre realizzato un sistema di *storage* a tre livelli con una capacità di 60 *terabyte raw* e l'acquisizione di 3 nuovi sistemi *server* idonei a fungere da *host* per l'infrastruttura virtuale, attualmente composta da 96 *core* fisici e 756 GB di memoria centrale, con 47 *server* virtuali attivi.

L'azione di consolidamento ha comportato la dismissione di 13 *server* fisici, con un abbattimento dei consumi elettrici (compresi quelli imputabili all'impianto di condizionamento) superiore al 50%.

Sicurezza informatica dell'Ufficio

Nel 2016 nessun evento relativo alla sicurezza ha prodotto danni o disservizi nel dominio dell'Ufficio. Nonostante la recrudescenza del fenomeno dello *spam* e del *phishing* tramite posta elettronica, 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 analoga, dal punto di vista quantitativo, a quella del 2015, con valori di *downtime* leggermente superiori alle nove ore complessive nell'arco dell'anno, dovuti a guasti e anomalie di tipo elettrico.

Attività di consulenza e cooperazione interna ed esterna

Il Dipartimento ha collaborato con le varie strutture dell'Autorità attraverso consulenze e approfondimenti sulle tematiche di interesse e, in particolare, in materia di nuove tecnologie e sicurezza informatica. Ha poi fornito osservazioni e indicazioni corredate dai necessari riferimenti tecnico-informatici e giuridici su tecnologie biometriche, tecnologie atte alla profilazione e alla geolocalizzazione anche in ambito lavorativo, tracciamento e rilevamento delle preferenze degli interessati, nonché individuazione dei relativi comportamenti di consumo.

Nell'ambito delle relazioni e delle comunicazioni che si sviluppano tramite la rete internet, ha fornito supporto alla comprensione delle dinamiche dei *social network*, dei motori di ricerca, delle *app* per *smartphone* e *tablet*, dell'Internet delle Cose (IoT) e, in generale, dei trattamenti di dati personali mediante le reti di comunicazione elettronica. In sede di istruttoria dei pareri resi dall'Autorità, il Dipartimento ha contribuito alla definizione del quadro attuativo del Sistema pubblico per l'identità digitale (SPID), con particolare riguardo agli aspetti di sicurezza delle comunicazioni nelle reti pubbliche. Per quanto riguarda lo sviluppo delle nuove tecnologie in ambito pubblico, ha fornito consulenza relativamente al trattamento dei dati personali nelle banche dati di interesse nazionale, specialmente in relazione all'Anagrafe tributaria, anche rispetto ai trattamenti svolti dagli intermediari privati, e all'Anpr.

Infine, il personale del Dipartimento ha assicurato la partecipazione agli impegni internazionali, in particolare nell'ambito del sottogruppo *Technology* del WP Art. 29 e del Gruppo di Berlino sulle telecomunicazioni (cfr. par. 24.5).

I dati statistici

IV - I dati statistici 2016

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	561
Pareri a Presidenza del Consiglio dei ministri e ministeri (art. 154, comma 4, del Codice)	20
Autorizzazioni generali al trattamento dei dati sensibili e giudiziari (art. 40 del Codice)	9
Autorizzazioni individuali al trattamento dei dati sensibili e giudiziari (art. 41 del Codice)	4
Provvedimenti concernenti trasferimenti di dati consentiti verso Paesi terzi (art. 44, comma 1, lett. *a*), del Codice)	12
Decisioni su ricorso (art. 145 del Codice)	277
Provvedimenti collegiali su segnalazioni e reclami (artt. 142-144 del Codice) nonché a seguito di accertamenti d'ufficio (art. 154 del Codice), nonché ai sensi degli artt. 10, comma 2, 13, comma 5, lett. *c*), 150, comma 5, del Codice	49
Ordinanze-ingiunzione adottate dal Garante	122
Riscontri a segnalazioni, reclami, richieste di parere e quesiti (artt. 142-144 del Codice e artt. 5 e 11, Reg. Garante n. 1/2007)	4.633
Provvedimenti collegiali su verifiche preliminari per trattamenti che presentano rischi specifici (art. 17 del Codice)	29
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)	2
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari (art. 154, comma 1, lett. *g*)	6
Ulteriori pareri resi a soggetti pubblici ai sensi dell'art. 154, comma 1, lett. *g*), del Codice)	8
Risposte ad atti di sindacato ispettivo e di controllo	9
Risposte a quesiti e altre istanze	24.097
Leggi regionali esaminate	11
Rilievi formulati in relazione a leggi regionali ai fini dell'impugnazione *ex* art. 127 Cost.	6
Accertamenti e controlli effettuati *in loco* (artt. 157-158 del Codice)	282
Violazioni amministrative contestate	2.339
Sanzioni applicate con ordinanza di ingiunzione	175
Pagamenti derivanti dall'attività sanzionatoria	€ 3.289.896
Comunicazioni di notizia di reato all'autorità giudiziaria	53
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	32
Ricorsi (trattati) *ex* art. 152 del Codice	12
Opposizioni (trattate) a provvedimenti del Garante	80
Notificazioni pervenute nell'anno 2016	2.369
Notificazioni pervenute dal 2004 al 31 dicembre 2016	29.059
Riunioni del Gruppo Art. 29	6
Partecipazione a sottogruppi di lavoro - Gruppo Art. 29	45
Riunioni autorità comuni di controllo (Europol, SIS II, Dogane, Eurodac, VIS)	16
Conferenze internazionali	3
Riunioni presso il CoE, OCSE e altri organismi internazionali	8
Riunioni e *workshop* presso Consiglio/Commissione e altri organismi UE	10
Quesiti, questionari e richieste di contributi provenienti da altre Autorità e Istituzioni	29

Tabella 1. Sintesi delle principali attività dell'Autorità

Attività di comunicazione dell'Autorità	
Comunicati stampa	37
Newsletter	13
Prodotti editoriali	2
Prodotti web	11

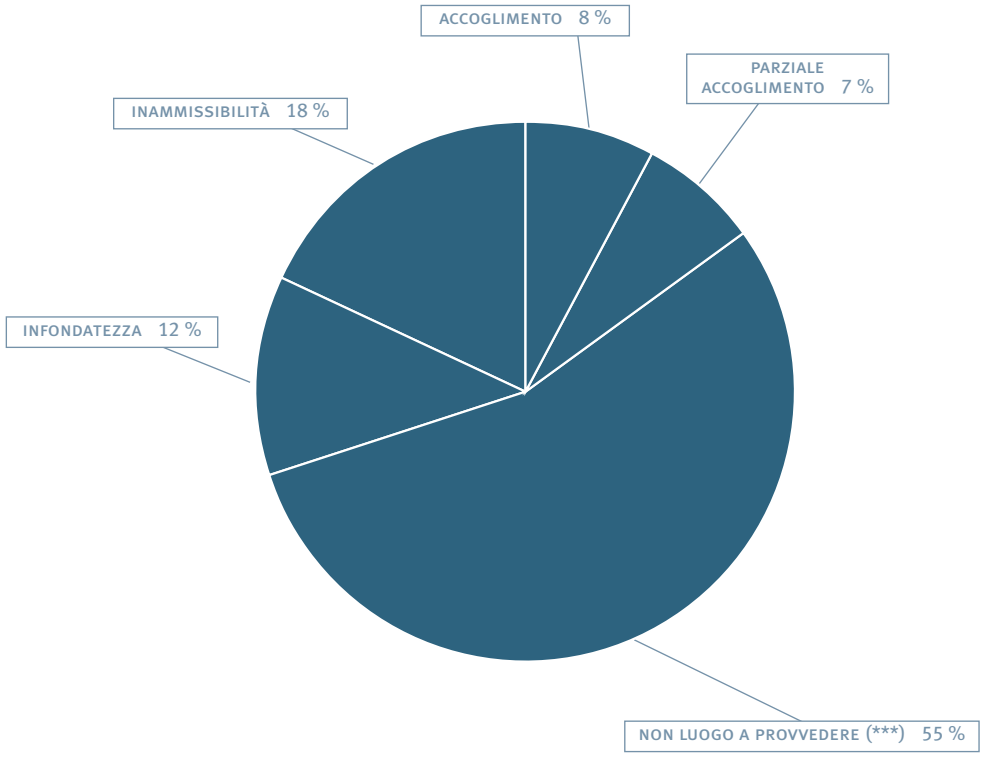
Tabella 2. Attività di comunicazione dell'Autorità

Tabella 3. Pareri *ex* art. 154, comma 4, del Codice

Pareri *ex* art. 154, comma 4, del Codice	
Temi	Riscontri resi nell'anno (*)
Informatizzazione e banche dati della p.a.	5
Attività di polizia, sicurezza nazionale e governo del territorio	2
Cad / Spid	2
Carta elettronica studenti/docenti	2
Fisco	3
Dati sanitari	6
Totale	**20**

Tabella 4. Tipologia delle decisioni su ricorsi

Decisioni su ricorsi	
Tipi di decisione (**)	**Numero ricorsi**
Accoglimento	22
Parziale accoglimento	20
Non luogo a provvedere (***)	153
Infondatezza	33
Inammissibilità	49
Totale	277



(*) Inerenti anche ad affari pervenuti anteriormente al 2016
(**) Le decisioni sui ricorsi possono contenere più statuizioni in base alle diverse richieste presentate: la statistica prende in esame, in tali casi, la statuizione più "favorevole" al ricorrente
(***) Casi nei quali le richieste del ricorrente sono state soddisfatte nel corso del procedimento

Categorie di titolari	
	Numero ricorsi
Banche e società finanziarie	71
Compagnie di assicurazione	7
Sistemi di informazioni creditizie	12
Centrale rischi Banca d'Italia e trattamenti presso archivio CAI	2
Società di informazioni commerciali	7
Amministrazioni pubbliche e concessionari di pubblici servizi	12
Strutture sanitarie pubbliche e private	5
Parrocchie	1
Fornitori telefonici e telematici	9
Attività di *marketing* svolta da imprenditori privati	9
Datori di lavoro pubblici e privati	33
Editori (anche televisivi)	86
Liberi professionisti	8
Amministrazioni condominiali	2
Associazioni	3
Altri	10
Totale	277

Tabella 5. Suddivisione dei ricorsi in relazione alle categorie di titolari del trattamento

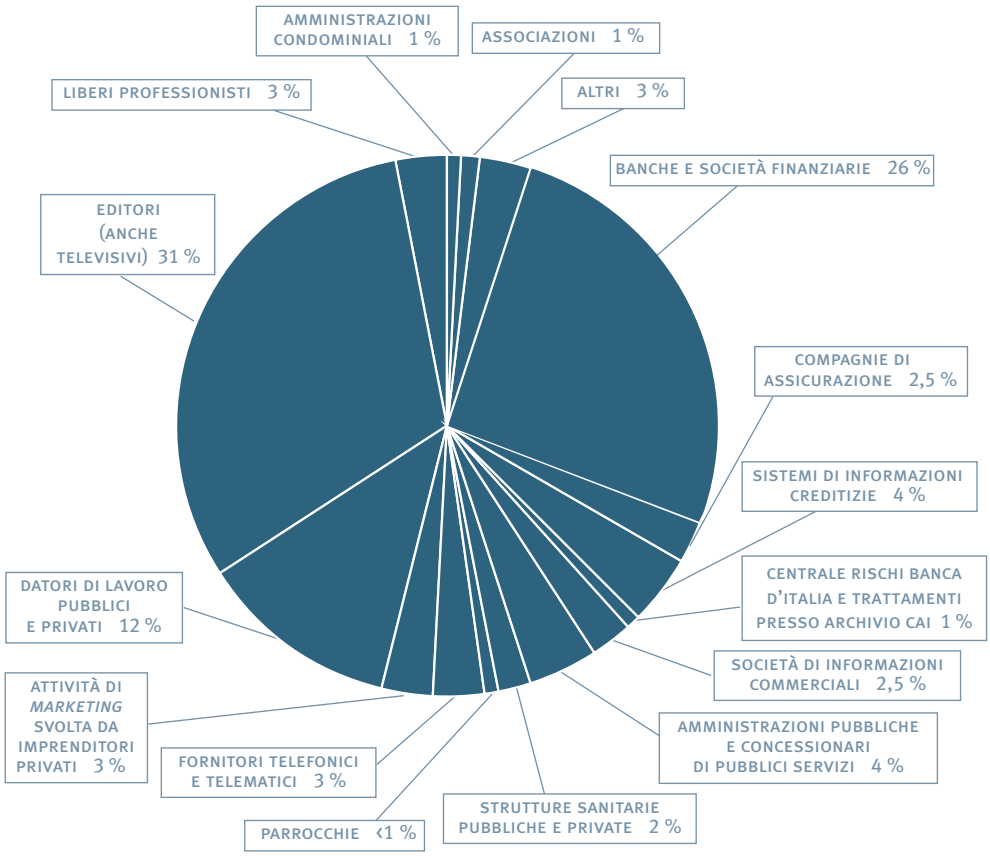
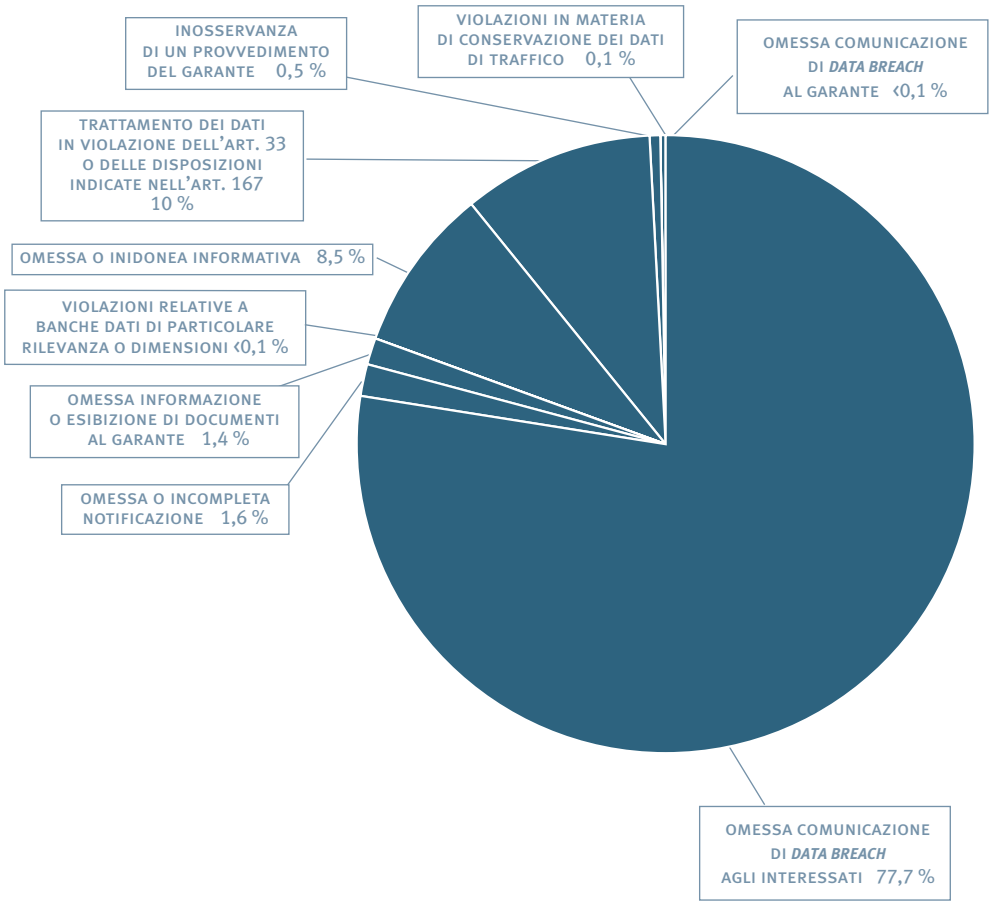


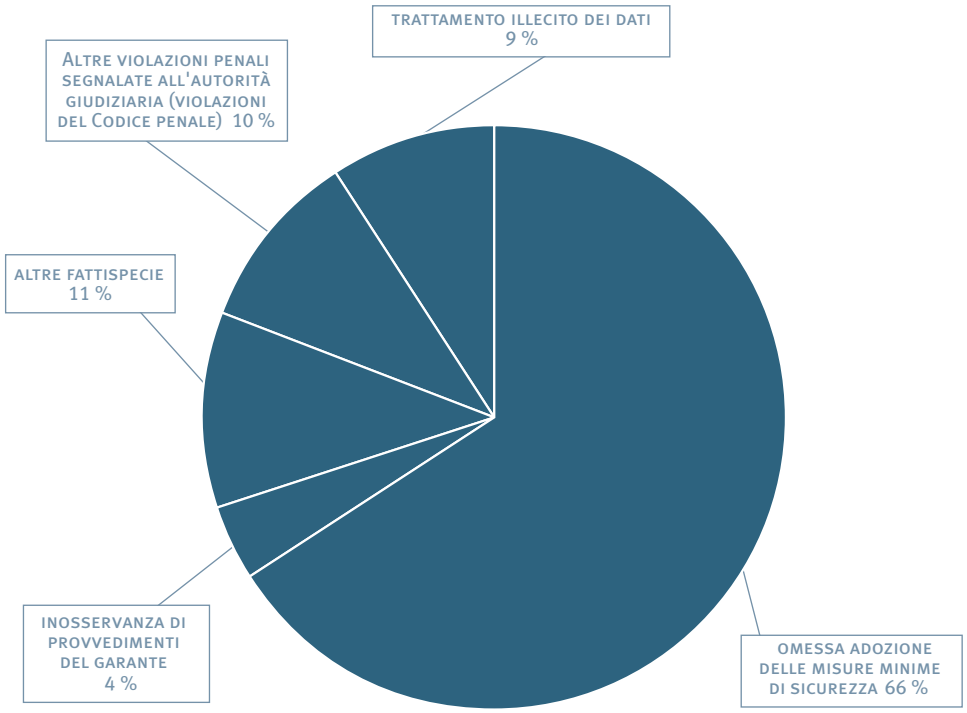
Tabella 6. Violazioni amministrative contestate

Violazioni amministrative contestate	
Omessa o inidonea informativa (art. 161 del Codice)	200
Trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis*, del Codice)	236
Inosservanza di un provvedimento del Garante (art. 162, comma 2-*ter*, del Codice)	11
Violazioni in materia di conservazione dei dati di traffico (art. 162-*bis,* del Codice)	3
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)	1.817
Omessa o incompleta notificazione (art. 163 del Codice)	37
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)	32
Violazioni relative a banche dati di particolare rilevanza o dimensioni (art. 164-*bis*, comma 2, del Codice)	2
Totale	**2.339**



Comunicazioni di notizia di reato all'autorità giudiziaria	
	Segnalazioni
Trattamento illecito dei dati (art. 167 del Codice)	5
Omessa adozione delle misure minime di sicurezza (art. 169 del Codice)	35
Inosservanza di provvedimenti del Garante (art. 170 del Codice)	2
Altre fattispecie (art. 171 del Codice)	6
Altre violazioni penali segnalate all'autorità giudiziaria (violazioni del codice penale)	5
Totale	**53**

Tabella 7. Comunicazioni di notizia di reato all'autorità giudiziaria



Pagamenti derivanti dall'attività sanzionatoria	
Somme versate a titolo di oblazione in via breve	2.324.440
Somme versate in conseguenza di ordinanze ingiunzione	432.976
Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169 del Codice)	150.000
Ulteriori entrate derivanti dall'attività sanzionatoria	382.480
Totale	**3.289.896**

Tabella 8. Pagamenti derivanti dall'attività sanzionatoria

Quesiti		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale quesiti	**394**	**300**

Tabella 9. Quesiti

(*) Inerenti anche ad affari pervenuti anteriormente al 2016

Tabella 10. Segnalazioni e reclami

Segnalazioni e reclami		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale segnalazioni e reclami	**7.969**	**4.333**
Temi principali		
Assicurazioni	50	37
Associazioni	57	49
Centrali rischi	152	122
Concessionari pubblici servizi	105	67
Condominio	30	23
Credito	243	224
Enti locali	106	106
Giornalismo e libertà d'espressione	232	113
Imprese	163	120
Informazioni commerciali	7	8
Internet	44	42
Istruzione	36	36
Lavoro	248	227
Marketing (posta cartacea, *e-mail*, fax, sms)	227	318
Marketing telefonico	5.580	2.355
Recupero crediti	138	144
Sanità e servizi di assistenza sociale	106	106
Videosorveglianza	272	204

Tabella 11. Atti di sindacato ispettivo e controllo

Atti di sindacato ispettivo e controllo	
Temi	Numero
Esercizio dei diritti fondamentali	3
Riservatezza delle comunicazioni	2
Trattamento di dati personali nell'attività di promozione commerciale svolta mediante *call center*	1
Dati sul web	1
Fisco	1
Videosorveglianza	1
Totale	**9**

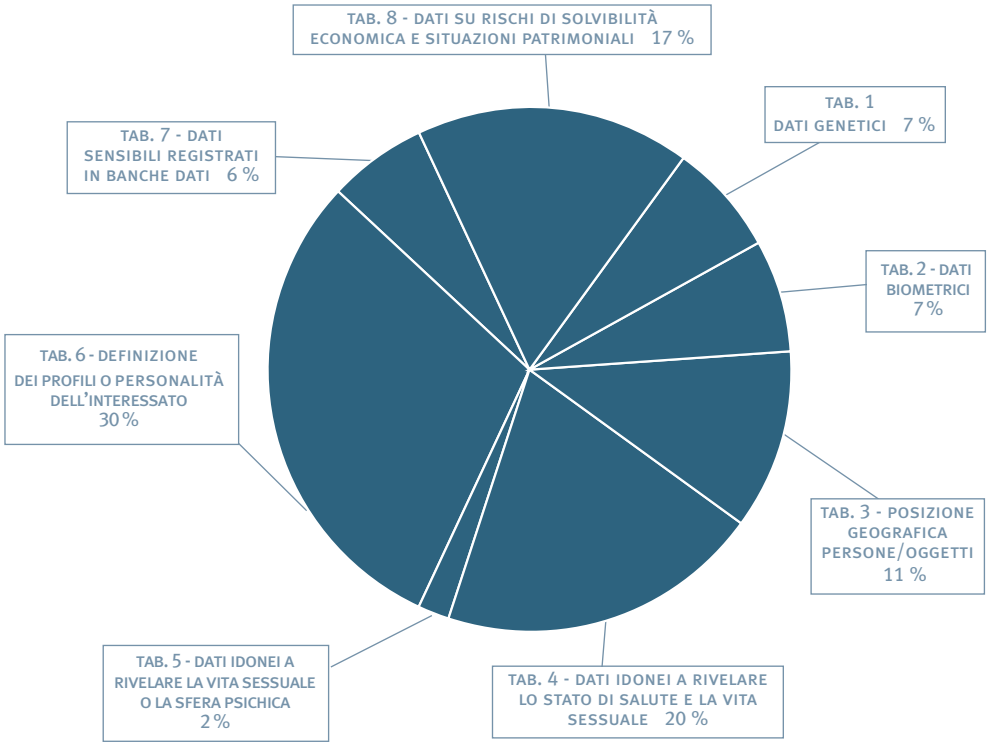
Tabella 12. Tipologie di notificazioni pervenute: 2004-2016

Tipologie di notificazioni pervenute: 2004-2016 (**)			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute (**)
Prima notificazione al Garante	1.306	21.320	22.626
Modifica di una precedente notificazione	209	4.833	5.042
Notificazione della cessazione del trattamento	117	1.274	1.391
Totale	**1.632**	**27.427**	**29.059**

(*) Inerenti anche ad affari pervenuti anteriormente al 2016
(**) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2016

Suddivisione delle notificazioni per tipologia di trattamento effettuato 2004-2016	
Tabelle di notificazione compilate (*)	Numero
Tabella 1 - Trattamento di dati genetici	3.126
Tabella 2 - Trattamento di dati biometrici	2.815
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	4.862
Tabella 4 - Trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, effettuato 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	8.581
Tabella 5 - Trattamento di dati idonei a rivelare la vita sessuale o la sfera psichica effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale	891
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	12.739
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	2.385
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	7.380
Totale (**)	**42.779**

Tabella 13. Suddivisione delle notificazioni per tipologia di trattamento effettuato 2004-2016



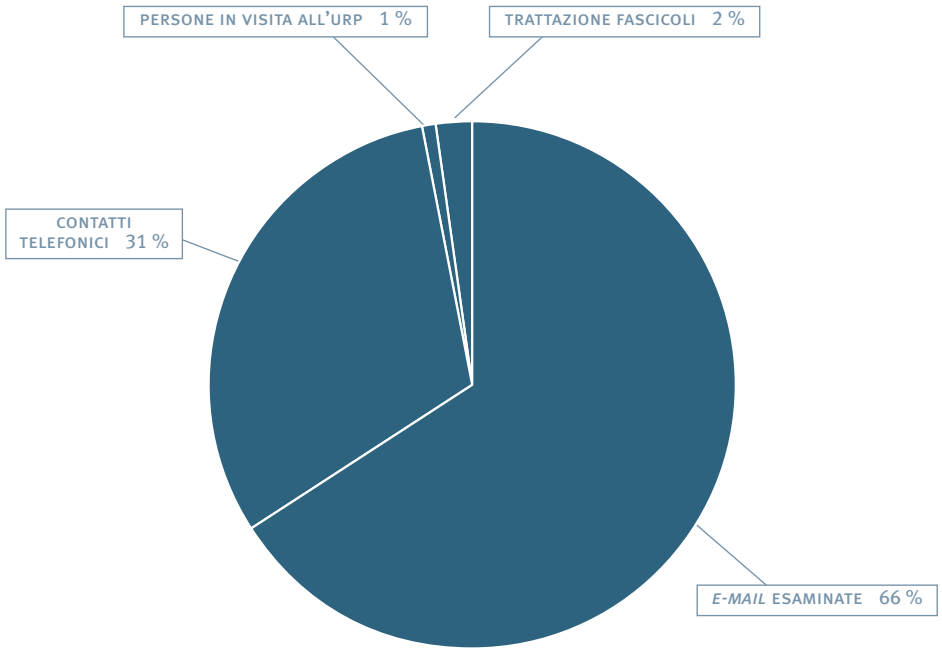
(*) Situazione alla data del 31 dicembre 2016
(**) N.B. Il totale è superiore alla sommatoria della precedente tabella in quanto una singola notificazione può riguardare più trattamenti

Tabella 14. Tipologie di notificazioni pervenute nel 2016

Tipologie di notificazioni pervenute nel 2016 (*)			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute (*)
Prima notificazione al Garante	50	1.499	1.549
Modifica di una precedente notificazione	29	543	572
Notificazione della cessazione del trattamento	28	220	248
Totale	**107**	**2.262**	**2.369**

Tabella 15. Ufficio relazioni con il pubblico

Ufficio relazioni con il pubblico	
	2016
E-mail esaminate	15.835
Contatti telefonici	7.550
Persone in visita all'Urp	268
Trattazione fascicoli	444
Totale	**24.097**



(*) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2016

Grafico 16. *E-mail* esaminate dall'Ufficio relazioni con il pubblico

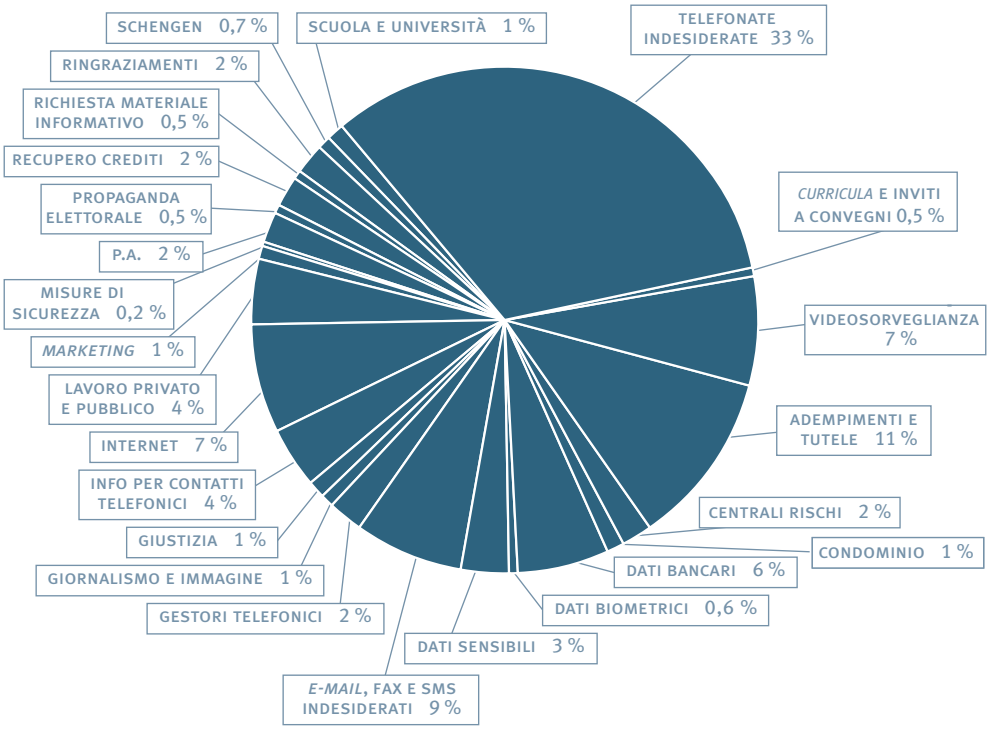


Tabella 17. Posti previsti in organico

Posti previsti in organico	
Segretario generale	1
Dirigenti	21
Funzionari	88
Operativi	26
Esecutivi	1
Totale	137
Personale a contratto	8

Tabella 18. Personale in servizio

Personale in servizio (*)				
Area	In ruolo (a)	In posizione di fuori ruolo (b)	Comandato presso altre amministrazioni o in aspettativa (c)	Impiegato dall'Ufficio (a+b-c)
Segretario generale	1	–	–	1
Dirigenti	13	2		15
Funzionari	71	4	2	73
Operativi	24			24
Esecutivi	–	–	–	–
Totali	**109**	**6**	**2**	**113**
Personale a contratto				8

Tabella 19. Risorse finanziarie

Risorse finanziarie						
Entrate accertate	**Anno 2016**		**Anno 2015**		**Variazione %**	
Entrate correnti		19.889.832		19.241.951		3,37%
di cui trasferimento dallo Stato per contributo ordinario	6.616.878		6.875.993		-3,77%	
Totale entrate		**19.889.832**		**19.241.951**		**3,37%**
Spese impegnate	**Anno 2016**		**Anno 2015**		**Variazione %**	
Spese di funzionamento		18.702.287		18.045.363		3,64%
Spese in conto capitale		138.640		414.296		-66,54%
Rimborsi al Mef		253.612		253.612		0,00%
Totale spese		**19.094.539**		**18.713.271**		**2,04%**

Valori: euro

(*) Situazione alla data del 31 dicembre 2016

Tabella 20. Attività internazionali dell'Autorità

Unione europea			
Gruppo Articolo 29	Sessione plenaria Art. 29		2 e 3 febbraio 12 e 13 aprile 7 e 8 giugno 25 luglio 27 e 28 settembre 12 e 13 dicembre
	Riunioni dei sottogruppi	*Border Travel Law Enforcement* (BTLE)	7 gennaio 15 marzo 12 maggio 15 novembre
		Cooperation	11 gennaio 9 marzo 18 maggio 25 maggio (*workshop*) 31 agosto-2 settembre (*workshop*) 4 novembre
		E-Government	14 gennaio 7 marzo 10 maggio 7 novembre
		Financial Matters	10 marzo 17 maggio 8 settembre 23 novembre
		Future of Privacy	12 gennaio 20 gennaio 30 marzo 17 maggio (*workshop*) 24 maggio 26 settembre (*workshop*) 22 novembre 30 novembre (*workshop "delisting"*)
		Key Provisions	10 marzo 28 aprile 23 giugno 10 novembre
		International Transfers	8 gennaio 16 marzo 11 maggio 17 novembre
		Technology	13 e 14 gennaio 8 e 9 marzo 18 e 19 maggio 4-5 luglio 19-20 ottobre
		EDPB IT Task Force	3 maggio 20 giugno 27 settembre 18 ottobre 16 novembre
		Enforcement	15 novembre

Unione europea	
Autorità di controllo comune EUROPOL	29 febbraio-4 marzo (ispezione) 17 e 18 maggio (NPG *meeting*) 9 e 10 giugno 22 e 23 settembre (NPG *meeting*) 4 ottobre 8 dicembre
Autorità di controllo comune DOGANE	10 giugno 9 dicembre
Gruppo di coordinamento della supervisione SID	9 dicembre
Gruppo di coordinamento della supervisione SIS II	14 aprile 22 novembre
Gruppo di coordinamento della supervisione EURODAC	15 aprile 23 novembre
Gruppo di coordinamento della supervisione VIS	15 aprile 23 novembre
Schengen *Committee* – Valutazione Italia – *report* protezione dei dati	6 ottobre
Eurojust	10-12 febbraio (ispezione) 15-16 dicembre

Unione europea		
Riunioni di gruppi di esperti	**Consiglio UE - Dapix**	9 marzo 10 marzo 14 marzo 23 maggio 29 novembre
Commissione UE – *e-Privacy Directive Revision*		19 aprile
ENISA *expert Group – Privacy Risk Assessment*		22 giugno
C- ITS *Intelligent Transport System* WG		19 ottobre 25 novembre 12 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	14 novembre 15-16 novembre
	Conference *call*	28 aprile 19 maggio 9 settembre 4 novembre
	Ministeriale OCSE 2016	20 – 24 giugno
	Ministerial Task Force Conference call	19 gennaio 16 febbraio 18 marzo 28 aprile
Consiglio d'Europa	Comitato Consultivo Convenzione 108/1981 (T-PD)	22 e 23 settembre
	T-PD *Bureau*	22-24 marzo 5-7 ottobre 30 novembre-2 dicembre
	Cahdata	15 e 16 giugno
Gruppi di lavoro specifici	Gruppo internazionale di lavoro sulla protezione dei dati nelle telecomunicazioni (IWGDPT)	25 e 26 aprile 22-23 novembre
International Enforcement	GPEN *(Global Privacy Enforcement Network – Sweep conference call)*	29 gennaio 15 marzo 31 agosto

Conferenze internazionali	
Conferenza di primavera delle Autorità europee di protezione dati	26 e 27 maggio, Budapest
37ª Conferenza internazionale delle Autorità di protezione dati	17-20 ottobre, Marrakech
Conferenza internazionale	7-8 novembre, Mosca

Altre conferenze e *meeting*	
CIPL *Dialogue on GDPR implementation and compliance - Workshop*	16 marzo, Amsterdam 19 settembre, Parigi
Sixth EDPD	25 e 26 aprile, Berlino
EAG *workshop*	31 maggio, Bruxelles
Annual Privacy Forum	7 e 8 settembre, Francoforte
CRISP *Workshop*	30 settembre, Madrid
FabLab	26 luglio, Bruxelles
Big Data and Anonymization Workshop	8-9 novembre, Bruxelles
Workshop Portability	22-23 novembre, Ispra

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

A TUTELA DI UN DIRITTO FONDAMENTALE

Redazione
Garante per la protezione dei dati personali

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

stampa:
Tipolitografia Ugo Quintily S.p.A.

1997
2017
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI
A TUTELA DI UN DIRITTO FONDAMENTALE