SENATO DELLA REPUBBLICA

XVII LEGISLATURA

Doc. **CXXXVI**
n. **2**

RELAZIONE

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

(Anno 2013)

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

Presentata dal Garante per la protezione dei dati personali

(SORO)

Trasmessa alla Presidenza il 12 giugno 2014

PAGINA BIANCA

In evidenza – 2013

Gennaio

Abbiamo prescritto l'adozione di idonei accorgimenti, anche tecnici, affinché le informazioni contenute in *dossier* sanitari siano nella disponibilità del solo professionista o della struttura che li ha redatti e possano essere condivisi con altri professionisti che abbiano in cura l'interessato presso altri reparti solo qualora lo stesso esprima uno specifico consenso, che può estendersi anche alle informazioni sanitarie relative a eventi clinici pregressi [par. 5.1.2]

. . . . . .

Abbiamo vietato il trattamento effettuato mediante l'impianto di videosorveglianza installato presso un esercizio commerciale della grande distribuzione a causa di violazioni della disciplina di protezione dei dati personali, di quella in materia di controlli a distanza dei lavoratori nonchè in ragione della mancanza di licenza prefettizia di guardia particolare giurata in capo al personale della società di vigilanza, incaricata di compiti anti-rapina e anti-taccheggio, cui l'impianto era stato affidato in gestione [par. 11.1]

Febbraio

Nella Giornata europea della *privacy*, abbiamo puntato i riflettori sul cyberbullismo. Sul sito del Garante è stato diffuso un video dedicato ai giovani con le istruzioni per un uso consapevole dei *social network* ed una nota è stata inviata al Ministro dell'istruzione per sensibilizzarlo sulla delicata tematica [par. 20.6]

. . . . . .

Nel dare parere favorevole allo schema di decreto legislativo del Ministro per la pubblica amministrazione e la semplificazione relativo agli obblighi di trasparenza della p.a., abbiamo segnalato alcune criticità (anche in relazione al quadro giuridico comunitario) e fornito indicazioni con l'obiettivo di garantire che la trasparenza non entri in conflitto con il diritto alla riservatezza e alla protezione dei dati (per esempio, evitando la diffusione di dati relativi alla salute o a condizioni di disagio economico e sociale di soggetti deboli che beneficiano di sussidi) [par. 3.2.2]

. . . . . .

Abbiamo vietato la diffusione su siti web istituzionali di numerosi comuni di ordinanze concernenti l'esecuzione di trattamenti sanitari obbligatori [par. 4.4]

. . . . . .

Quale ulteriore azione di contrasto del *telemarketing* cd. selvaggio e delle offerte promozionali indesiderate, abbiamo effettuato accertamenti ispettivi ed emesso ordinanze ingiunzione nei confronti di due importanti società di servizi informatici, specializzate nel settore delle banche dati, condannate al pagamento di rilevanti sanzioni per aver violato provvedimenti prescrittivi già adottati nei loro confronti [par. 10.3]

Marzo

Abbiamo reso un parere al Ministero dell'economia e delle finanze su uno schema di decreto ministeriale relativo al funzionamento del sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con particolare riferimento al furto d'identità, con il quale, oltre a chiedere il rispetto del principio di finalità e l'adozione di misure di sicurezza adeguate, si è ravvisata la necessità di precisare nel regolamento i diversi livelli di accesso al sistema da parte dei cd. aderenti diretti e indiretti nonché l'opportunità di prevedere modalità di informazione a vantaggio degli interessati delle eventuali incongruenze dei dati riscontrati nelle banche dati pubbliche all'esito delle verifiche effettuate [par. 3.2.2]

. . . . . .

Avvalendoci della Guardia di finanza, abbiamo effettuato accertamenti ispettivi nei confronti di 11 società di telefonia e *provider* sul rispetto delle norme per la conservazione dei

dati di traffico telefonico e telematico, comminando le sanzioni previste dal Codice nei casi di mancato rispetto delle precedenti prescrizioni dell'Autorità [par. 10.2]

. . . . . .

Abbiamo reso un parere sullo schema di accordo tra il Governo, le Regioni e le Province autonome di Trento e di Bolzano sulle linee guida per la ricognizione dell'utilizzo di cellule e tessuti umani (cornee, cute, valvole cardiache) per trapianti sperimentali e per nuovi medicinali per terapie avanzate chiedendo l'utilizzo di dati aggregati al fine di escludere il rischio di identificazione, anche indiretta, dei pazienti coinvolti [par. 5.2]

Aprile

Abbiamo adottato un provvedimento generale in attuazione della disciplina sulla comunicazione delle violazioni di dati personali fornendo indicazioni in ordine ai soggetti interessati dai nuovi obblighi normativi, alle misure in grado di garantire un livello minimo comune di sicurezza, ai tempi e ai contenuti delle segnalazioni relative ai cd. *data breach*, per le quali è anche possibile utilizzare un modello disponibile sul sito dell'Autorità [par. 10.9]

Maggio

Abbiamo prescritto alle aziende sanitarie che utilizzano sistemi di videosorveglianza all'interno dei propri servizi igienici per accertare l'assenza di tossicodipendenza, di adottare misure e garanzie a tutela della riservatezza di quanti sono sottoposti alla raccolta dei campioni di urina, vietando, in particolare, la registrazione delle immagini con qualsiasi mezzo [par. 5.1]

. . . . . .

Abbiamo ritenuto sproporzionato l'impiego di dati biometrici per finalità di rilevazione delle presenze di insegnanti e personale tecnico-amministrativo in alcuni istituti scolastici [par. 11.2]

In un'ottica di semplificazione, abbiamo chiarito come il titolare del trattamento che, in ambito privato, acquisisce il consenso degli interessati per le finalità di *marketing* diretto tramite modalità automatizzate di contatto, possa effettuare il medesimo trattamento anche mediante modalità tradizionali, come la posta cartacea o le chiamate telefoniche tramite operatore, sempreché non venga esercitato nei suoi confronti il diritto di opposizione al trattamento [par. 10.7]

. . . . . .

Abbiamo predisposto un *vademecum* su "La *privacy* dalla parte dell'impresa - Dieci pratiche aziendali per migliorare il proprio *business*" che contiene pochi ma fondamentali consigli pratici per il rispetto delle regole poste a protezione dei dati personali [par. 20.4]

. . . . . .

A tutela della riservatezza, del libero sviluppo della personalità dei bambini, della spontaneità del rapporto con gli insegnanti nonché della libertà di insegnamento, abbiamo vietato l'uso di *webcam* in un asilo nido [par. 12.4]

Giugno

Abbiamo vietato ad una questura il trattamento delle immagini rilevate attraverso telecamere di sorveglianza che, istallate in strada per motivi di sicurezza pubblica, consentivano la visione diretta degli interni di private abitazioni [par. 8.2.1]

Luglio

Abbiamo prescritto, dandone comunicazione a Regioni, Province autonome e Inps, che, in occasione del rilascio della copia del verbale di invalidità per gli usi consentiti dalla legge (come richiedere il contrassegno per l'accesso alla Ztl o usufruire delle agevolazioni fiscali previste per l'acquisto di veicoli), le commissioni mediche omettano la descrizione dell'anamnesi, dell'esame obiettivo e della diagnosi del paziente [par. 5.2]

Abbiamo adottato le linee guida in materia di attività promozionale e contrasto allo *spam*, soffermandoci sulle nuove frontiere dello *spamming* – come quello diffuso sui *social network* (il cosiddetto *social spam*) o effettuato tramite alcune pratiche di "*marketing* virale" o "*marketing* mirato" – che possono comportare modalità più insidiose e invasive della sfera personale degli interessati [par. 10.10], nonché diffuso sul sito dell'Autorità una scheda informativa (*Spam: come difendersi*) e, anche su You-Tube, un video-tutorial

Abbiamo prescritto misure e accorgimenti, di natura fisica ed informatica, per incrementare la sicurezza dei dati personali raccolti e usati nello svolgimento delle intercettazioni da parte dei Centri Intercettazioni Telecomunicazioni (C.I.T.) situati presso ogni Procura della Repubblica e presso gli uffici di polizia giudiziaria delegati all'attività di intercettazione [par. 4.11]

Settembre

Abbiamo consentito a due banche di dotare i propri promotori finanziari di *tablet* in grado di analizzare i dati biometrici della sottoscrizione apposta dai clienti che intendono stipulare contratti finanziari in forma elettronica, prescrivendo contestualmente alle società coinvolte nell'abilitazione e nella gestione dei due sistemi l'adozione di particolari misure a tutela dei dati raccolti e di misure volte a garantire comunque ai clienti la possibilità di sottoscrivere i contratti anche attraverso modalità tradizionali [par. 12.5]

Ottobre

Abbiamo inviato una lettera al Presidente del Consiglio dei Ministri invitandolo a sostenere con forza, in seno al Consiglio dell'Unione europea, l'adozione del progetto di riforma del quadro normativo europeo in materia di protezione dei dati personali, rafforzandone il disegno complessivo, manifestando preoccupazione nei confronti delle attività di spionaggio della NSA con riguardo alle comunicazioni telefoniche e telematiche concernenti anche cittadini italiani [par. 8.4]

Abbiamo vietato l'inoltro alla clientela di comunicazioni telefoniche preregistrate senza l'intervento di un operatore per finalità di recupero crediti [par. 12.1]

Abbiamo formulato osservazioni all'Ivass, in relazione al tema della prevenzione e del contrasto alle frodi nel settore delle assicurazioni Rc auto, in merito alla banca dati dei sinistri e alle neocostituite anagrafe testimoni e anagrafe danneggiati, raccomandando di informare gli interessati (parti coinvolte nel sinistro, testimoni, *etc.*), di limitare a 5 anni il tempo di conservazione dei dati identificativi che li riguardano, di limitare la consultazione della banca dati ai soggetti indicati dalla legge al solo scopo di rendere più efficace la prevenzione e il contrasto alle frodi assicurative [par. 12.2]

A seguito di verifiche a campione, abbiamo accertato l'illiceità di numerosi trattamenti effettuati, nei confronti di lavoratori e clienti, mediante sistemi di videosorveglianza nel settore della grande distribuzione [par. 11.1]

Abbiamo prescritto misure a tutela degli interessati in caso di utilizzo, per le attività di *customer care* o *telemarketing*, di *call center* situati in Paesi dove non sono assicurate le garanzie previste dalla normativa europea di protezione dei dati. Tra le misure prescritte, oltre ad una completa informativa, anche l'obbligo per le società che si avvalgono dei *call center*, di darne previa comunicazione al Garante, utilizzando un modello disponibile sul sito, per permettere all'Autorità di valutare la portata del trasferimento dei dati personali al di fuori dell'Unione europea [par. 10.5]

A seguito di una verifica preliminare richiesta dalla Soprintendenza Speciale per i be-

ni archeologici di Napoli e Pompei, abbiamo accordato tempi più lunghi di conservazione delle immagini raccolte tramite il sistema di videosorveglianza dei cantieri e delle aree di stoccaggio del *Grande Progetto Pompei* con lo scopo di supportare l'attività della Prefettura volta a controllare, soprattutto a fini di prevenzione antimafia, la regolarità degli accessi e delle presenze in cantiere [par. 4.8]

. . . . . .

Abbiamo predisposto un *vademecum* su "Il condominio e la *privacy*" che prende in esame e fornisce indicazioni rispetto ai casi che più frequentemente emergono nelle relazioni condominiali [par. 20.4]

Novembre

Il Garante ha siglato un protocollo d'intenti con il Dipartimento delle informazioni per la sicurezza (Dis) della Presidenza del Consiglio dei Ministri volto a disciplinare alcune procedure informative funzionali all'esercizio delle rispettive attribuzioni, con particolare riferimento alle modalità di informazione idonee a consentire all'Autorità di conoscere alcuni elementi essenziali del trattamento dei dati personali effettuato dagli Organismi per l'informazione e la sicurezza in alcuni contesti peculiari, segnatamente quelli concernenti la sicurezza cibernetica o gli accessi alle banche dati delle pp.aa. o degli esercenti servizi di pubblica utilità [par. 8.4]

. . . . . .

Abbiamo impartito prescrizioni alle aziende sanitarie circa le corrette modalità di consegna a domicilio di presidi sanitari, a tutela della riservatezza e della dignità dei pazienti [par. 5.1]

. . . . . .

In coincidenza con un ricorso proposto dinanzi dell'Autorità, volto ad ottenere la deindicizzazione dai motori di ricerca del testo di un'interrogazione parlamentare contenente dati giudiziari (molto risalenti nel tempo e superati da successivi sviluppi processuali), i competenti organi della Camera dei deputati hanno adottato apposite disposizioni procedurali interne che, recependo linee interpretative e metodologiche già utilizzate in contesti simili (deindicizzazione di notizie disponibili negli archivi storici *online* delle principali testate giornalistiche), hanno offerto anche a queste particolari fattispecie una tutela adeguata [par. 16.4]

. . . . . .

Abbiamo effettuato un'approfondita verifica preliminare sui trattamenti effettuati dall'Agenzia delle entrate in relazione al cd. redditometro, fornendo prescrizioni in ordine ai numerosi profili di criticità (derivanti, peraltro, anche dallo stesso decreto ministeriale di attuazione del nuovo redditometro) relativi: alla qualità ed esattezza dei dati utilizzati dall'Agenzia; all'individuazione in via presuntiva della spesa sostenuta da ciascun contribuente riguardo ad ogni aspetto della vita quotidiana (tempo libero, libri, pasti fuori casa, *etc.*) mediante l'attribuzione alla generalità dei soggetti censiti nell'Anagrafe tributaria della spesa media rilevata dall'Istat; all'informativa da rendere al contribuente [par. 4.7]

Dicembre

Abbiamo avviato una consultazione pubblica sul trattamento di dati personali effettuati per pagamenti via *smartphone* e *tablet* e, più in generale, nell'ambito dei servizi di *mobile remote payment* [par. 10.8]

. . . . . .

Abbiamo vietato i trattamenti di dati personali relativi ad oltre 400 mila aspiranti lavoratori effettuati tramite un sito web per finalità di intermediazione tra domanda ed offerta di lavoro in violazione della disciplina di settore e di protezione dei dati personali [par. 11.3]

Indice

PAGINA BIANCA

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

II - L'ATTIVITÀ SVOLTA DAL GARANTE

III - L'UFFICIO DEL GARANTE

21. La gestione amministrativa dell'Ufficio

Elenco delle abbreviazioni più ricorrenti

La presente Relazione è riferita al 2013 e contiene talune notizie già anticipate nella precedente edizione nonché informazioni relative a sviluppi che si è ritenuto opportuno menzionare.

ad es.	ad esempio
AgID	Agenzia per l'Italia Digitale
Asl	Azienda sanitaria locale
Asp	Azienda sanitaria provinciale
art.	articolo
c.c.	codice civile
c.p.	codice penale
c.p.c.	codice procedura civile
c.p.p.	codice procedura penale
Cad	codice dell'amministrazione digitale
cap.	capitolo
cd.	cosiddetto
cfr.	confronta
cit.	citato
Codice	Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196)
Cost.	Costituzione
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
G.U.	Gazzetta Ufficiale della Repubblica italiana
G.U.U.E	Gazzetta Ufficiale dell'Unione europea
Gruppo Art. 29	Gruppo dei garanti europei previsto dall'art. 29 della direttiva 95/46/CE
l.	legge
lett.	lettera
n.	numero
p.	pagina
p.a.	pubblica amministrazione
pp.aa.	pubbliche amministrazioni
par.	paragrafo
provv.	provvedimento del Garante per la protezione dei dati personali
r.d.	regio decreto
reg.	regolamento
t.u.	testo unico
v.	vedi

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

PAGINA BIANCA

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

1 Introduzione: i principali interventi dell'Autorità nel 2013

Da una ricognizione, pur sommaria, dell'attività svolta nel corso del 2013 emerge la conferma di una delle caratteristiche di fondo del Garante (e quindi della sua attività), entrata ormai a far parte del dna dell'Autorità: quella di (dover) operare, in presa diretta, in tutti gli ambiti, i più vari, nei quali i flussi informativi incidono sulla vita delle persone, quali che siano i ruoli sociali di volta in volta rivestiti (cittadino, consumatore, lavoratore, paziente, *etc.*), in una tensione continua tra la dimensione sociale dell'individuo, che favorisce e talora impone la circolazione delle informazioni personali (anche sensibili), e la necessità che la dignità della persona e le sue libertà fondamentali trovino piena affermazione e un elevato livello di protezione. Per una conferma, se mai ve ne fosse la necessità, basta scorrere il contenuto dei provvedimenti "in evidenza", alcuni tra i tanti adottati nel periodo preso in considerazione, sovente a seguito delle attività ispettive effettuate dall'Autorità (cfr. par. 18.4), che sono riportati in apertura del volume (cfr. altresì, per un grado maggiore di dettaglio, i dati statistici contenuti nella sez. IV).

1.1. Il fronte dell'evoluzione tecnologica, specie nel settore delle comunicazioni elettroniche, e delle correlate potenzialità di sorveglianza dell'individuo che ne fa uso – anche indipendentemente dai confini nazionali, come segnalato nella lettera che il Garante ha inviato al Presidente del Consiglio dei Ministri, manifestando inquietudine nei confronti delle attività di spionaggio della *National Security Agency* in relazione alle comunicazioni telefoniche e telematiche concernenti altresì i cittadini italiani (par. 8.4) – resta al centro delle preoccupazioni dell'Autorità; anche per questa ragione, in presenza di elementi che rendono evidente un controllo crescente di fasce ampie della popolazione (e la conservazione di grandi masse di informazioni), nella stessa comunicazione al Governo è stato espresso un fermo invito a sostenere con forza, in seno al Consiglio dell'Unione europea, la necessità che quest'ultima adotti il progetto di riforma del quadro normativo europeo in materia di protezione dei dati personali, rafforzandone il disegno complessivo; obiettivo rispetto al quale l'Autorità, stimandone il rilievo, si è impegnata a fondo, nell'ambito delle proprie attribuzioni, anche nel corso del 2013 (cfr. par. 19.1). Sull'onda del cd. *Datagate*, il Garante è stato audito (ai sensi dell'art. 31, comma 3, l. n. 124/2007) dal Comitato parlamentare per la sicurezza della Repubblica (Copasir) e, quindi, l'11 novembre 2013, ha siglato un protocollo d'intenti con il Dipartimento delle informazioni per la sicurezza (Dis)

della Presidenza del Consiglio dei Ministri volto a disciplinare alcune procedure informative funzionali all'esercizio delle rispetrive attribuzioni, con particolare riferimento alle modalità di informazione idonee a consentire all'Autorità di conoscere alcuni elementi essenziali del trattamento dei dati personali effettuato dagli Organismi per l'informazione e la sicurezza in alcuni contesti peculiari, segnatamente quelli concernenti la sicurezza cibernetica e gli accessi alle banche dati delle pp.aa. o degli esercenti servizi di pubblica utilità (par. 8.4).

E affinché ciascuno possa trarre il massimo vantaggio dalla ricchezza informativa e dalle molteplici forme di partecipazione che internet consente, il Garante ha voluto dedicare alla vita in rete, segnatamente al tema del cyberbullismo, la Giornata europea della *privacy*: per rendere avvertiti gli utenti, anzitutto i giovani, dei pericoli connessi ad un uso non sempre consapevole (che talora sfocia nell'abuso) dei *social network*, ma sensibilizzando in pari tempo le istituzioni, in particolare il Ministro dell'istruzione, sulla delicata tematica (cfr. par. 20.6).

I comportamenti in rete sono rientrati anche nell'attività provvedimentale del Garante: il fenomeno dello *spam*, da anni oggetto di attenzione ed intervento da parte dell'Autorità, ha assunto forme nuove di manifestazione – si pensi a quello diffuso sui *social network* (il cosiddetto *social spam*) o effettuato tramite alcune pratiche di "*marketing* virale" o "*marketing* mirato" – sì da richiedere un aggiornato intervento con le linee guida formulate dal Garante (par. 10.10). La deindicizzazione di notizie disponibili negli archivi storici *online* delle principali testate giornalistiche, misura da tempo indicata dall'Autorità al fine di contemperare i diritti della persona (in particolare il rispetto del diritto all'identità personale) con la libertà di manifestazione del pensiero, continua a mostrare la sua validità, tanto che gli stessi organi della Camera dei deputati hanno recepito tale orientamento, adottando apposite disposizioni procedurali interne per offrire una tutela adeguata anche nei casi relativi a interrogazioni parlamentari contenenti informazioni oramai "datate" (cfr. par. 16.4).

Per conoscere in profondità il fenomeno dei pagamenti via *smartphone* e *tablet* e, più in generale, effettuati nell'ambito dei servizi di *mobile remote payment* è stata avviata una consultazione pubblica (par. 10.8).

1.2. Sempre con riferimento alla rete, nel dare parere favorevole allo schema di decreto legislativo relativo agli obblighi di trasparenza della p.a. che, nella prospettiva del (successivamente adottato) d.lgs. 14 marzo 2013, n. 33 (sulla scia di precedenti interventi normativi), proprio su internet – per il tramite dei siti web istituzionali delle amministrazioni – trovano il luogo privilegiato di esplicazione, il Garante ha segnalato alcune criticità (anche in relazione al quadro normativo comunitario e agli orientamenti formulati dalla Corte di Giustizia dell'Unione europea) e fornito indicazioni, solo in parte accolte, con l'obiettivo di garantire che la trasparenza non entri in conflitto con il diritto alla riservatezza e alla protezione dei dati personali (per esempio, evitando la diffusione di dati relativi alla salute o a condizioni di disagio economico e sociale di soggetti deboli che beneficiano di sussidi) (par. 3.2.2). Deve a questo proposito segnalarsi con preoccupazione il fenomeno della pubblicazione in internet, spesso per il tramite dell'albo pretorio *online*, di dati sensibili – si pensi al caso della diffusione di ordinanze concernenti l'esecuzione di trattamenti sanitari obbligatori su siti web istituzionali di numerosi comuni (par. 4.4) – o comunque eccedenti, riferiti a individui e pubblici dipendenti (par. 11.5), rispetto al quale il Garante è intervenuto con provvedimenti di divieto.

1.3. I chiaroscuri della rete, tuttavia, rappresentano solo una parte dell'area di intervento dell'Autorità, peraltro reso oltremodo difficile dai limiti geografici del-

l'ambito di applicazione della disciplina di protezione dei dati personali (limite che la proposta di regolamento generale sulla protezione dei dati in discussione tenta di superare facendo rientrare nell'ambito di applicazione della stessa anche il trattamento dei dati personali di residenti nell'Unione effettuato in relazione all'offerta di beni o alla prestazione di servizi agli stessi o per controllarne il comportamento ancorché effettuato da soggetti stabiliti in Paesi terzi). Rimane, infatti, costante l'attenzione – peraltro desumibile dal significativo incremento dei procedimenti sanzionatori amministrativi (par. 18.5.2) – nei confronti di altri trattamenti che in profondità possono incidere sui diritti delle persone, anzitutto quelli effettuati con dati sensibili e giudiziari, rispetto ai quali il Garante ha rinnovato il 12 dicembre 2013 le autorizzazioni generali al trattamento (pubblicate in G.U. 27 dicembre 2013, n. 302). Entro questa cornice, formano oggetto di frequente segnalazione operazioni improprie di trattamento di dati personali concernenti le condizioni di salute degli interessati, sia nel contesto sanitario che al di fuori di esso. Intervenendo in quest'area, il Garante ha così prescritto l'adozione di idonei accorgimenti, anche tecnici, affinché le informazioni contenute in *dossier* sanitari siano nella disponibilità del solo professionista o della struttura che li ha redatti e possano essere condivisi con altri professionisti che abbiano in cura l'interessato presso altri reparti solo qualora il paziente esprima uno specifico consenso, che può estendersi anche alle informazioni sanitarie relative a eventi clinici pregressi; più in generale, costante è l'attenzione dedicata alle problematiche legate alla realizzazione a livello nazionale del Fascicolo sanitario elettronico (par. 5.1.2).

Prescrizioni sono state poi impartite alle aziende sanitarie che utilizzano sistemi di videosorveglianza all'interno dei propri servizi igienici per accertare l'assenza di tossicodipendenza, affinché siano adottate misure e garanzie a tutela della riservatezza di quanti sono sottoposti alla raccolta dei campioni di urina, vietando, in particolare, la registrazione delle immagini con qualsiasi mezzo e, analogamente, misure e accorgimenti sono stati individuati affinché, nella vita di ogni giorno, le aziende sanitarie adottino corrette modalità di consegna a domicilio di presìdi sanitari, a tutela della riservatezza e della dignità dei pazienti (par. 5.1). In questa stessa prospettiva, con provvedimento generale, oggetto di ampia comunicazione (anche a Regioni, Province autonome e Inps), è stato prescritto che, quando le commissioni mediche rilasciano copia del verbale di invalidità per gli usi consentiti dalla legge (come richiedere il contrassegno per l'accesso a zone a traffico limitato o per usufruire delle agevolazioni fiscali previste per l'acquisto di veicoli), vengano omesse le parti con la descrizione dell'anamnesi, dell'esame obiettivo e della diagnosi del paziente (par. 5.2).

Né si esaurisce nell'attività di prescrizione e controllo l'azione del Garante con riguardo al trattamento dei dati riferiti alle condizioni di salute: intensa è la cooperazione prestata dall'Autorità anche in questo settore (cfr. par. 3.2), sia partecipando a tavoli di lavoro, sia adottando pareri, al fine di assicurare che i trattamenti siano posti in essere nel rispetto della dignità e della riservatezza degli interessati. In questa prospettiva è stato reso un parere sullo schema di accordo tra il Governo, le Regioni e le Province autonome di Trento e di Bolzano sulle linee guida per la ricognizione dell'utilizzo di cellule e tessuti umani (cornee, cute, valvole cardiache) per trapianti sperimentali e per nuovi medicinali per terapie avanzate, chiedendo l'utilizzo di dati aggregati al fine di escludere il rischio di identificazione anche indiretta dei pazienti coinvolti (par. 5.2).

1.4. In tema di grandi banche dati, l'Autorità ha mantenuto un faro acceso anche sul fronte della conservazione dei dati di traffico – peraltro oggetto di un recente, rimarchevole intervento da parte della Corte di Giustizia dell'Unione euro-

pea dell'8 aprile 2014 (*Digital Rights Ireland* e *Seitlinger and Others*, Cause riunite C-293/12, C-594/12) sulla normativa europea in materia (i cui effetti si spiegheranno sugli ordinamenti dei Paesi membri) – effettuando, mediante la collaborazione della Guardia di finanza, accertamenti ispettivi a campione sul rispetto delle misure prescritte dal Garante, già nel 2008, per la conservazione dei dati di traffico telefonico e telematico e comminando, nei casi di violazioni riscontrate, le sanzioni previste dal Codice (cfr. par. 10.2).

E ancora, rimanendo nel settore delle comunicazioni elettroniche, con un provvedimento generale in attuazione della disciplina sulla comunicazione delle violazioni di dati personali, il Garante ha fornito indicazioni in ordine ai soggetti interessati dai nuovi obblighi normativi dettati dagli artt. 32 e 32-*bis* del Codice, alle misure in grado di garantire un livello minimo comune di sicurezza, ai tempi e ai contenuti delle segnalazioni relative ai cd. *data breach* per le quali è anche possibile utilizzare un modello disponibile sul sito dell'Autorità (par. 10.9).

1.5. Se la videosorveglianza continua a formare oggetto di esame ed intervento da parte dell'Autorità, sia in ambito pubblico (par. 4.8) che privato (par. 12.4), merita, per la particolarità delle fattispecie considerate, menzionare il divieto indirizzato ad un asilo nido rispetto all'utilizzo di *webcam*, a tutela della riservatezza e del libero sviluppo della personalità dei bambini, della spontaneità del rapporto con gli insegnanti nonché della libertà di insegnamento (par. 12.4), ed il via libera (previa adozione di adeguate garanzie individuate dall'Autorità all'esito di una verifica preliminare richiesta da un Comune) all'installazione di un sistema di videosorveglianza "intelligente" volto a contrastare atti di vandalismo mediante la comparsa, in tempo reale, di un allarme sul monitor della postazione di controllo in caso di permanenza prolungata di un soggetto nelle aree adiacenti monumenti e sedi istituzionali (par. 4.8).

Il bilanciamento tra sicurezza e diritti fondamentali degli interessati ha formato oggetto di intervento del Garante anche in altre forme: è stato, ad esempio, vietato ad una questura il trattamento delle immagini rilevate attraverso telecamere di sorveglianza che, istallate sulla strada per motivi di pubblica sicurezza, consentivano però la visione diretta degli interni di private abitazioni (par. 8.2.1); a seguito di una verifica preliminare richiesta dalla Soprintendenza Speciale per i beni archeologici di Napoli e Pompei, sono stati accordati tempi più lunghi di conservazione delle immagini raccolte tramite il sistema di videosorveglianza dei cantieri e delle aree di stoccaggio del "Grande Progetto Pompei" con lo scopo di supportare l'attività della Prefettura volta a controllare, soprattutto a fini di prevenzione antimafia, la regolarità degli accessi e delle presenze in cantiere (par. 4.8).

Da segnalare altresì le misure e gli accorgimenti, di natura fisica ed informatica, individuati in un importante provvedimento prescrittivo volto ad incrementare la sicurezza dei dati personali raccolti e usati nello svolgimento delle intercettazioni da parte dei Centri Intercettazioni Telecomunicazioni (C.I.T.) situati presso ogni Procura della Repubblica e presso gli uffici di polizia giudiziaria delegata all'attività di intercettazione (par. 4.11).

1.6. L'Autorità, in una prospettiva di semplificazione da tempo perseguita, ha predisposto un *vademecum* su "Il condominio e la *privacy*" ed uno dedicato a "La *privacy* dalla parte dell'impresa - Dieci pratiche aziendali per migliorare il proprio *business*", che contengono pochi ma fondamentali consigli pratici per il rispetto delle regole poste a protezione dei dati personali al fine di favorirne una corretta attuazione (par. 20.4).

Il Garante ha altresì chiarito, in un settore rispetto al quale forte è la sensibilità da parte del pubblico e in un'ottica di semplificazione, come tutti i titolari del trattamento che, in ambito privato, acquisiscono il consenso degli interessati per le finalità di *marketing* diretto tramite modalità automatizzate di contatto, possano effettuare il medesimo trattamento anche mediante forme tradizionali, come la posta cartacea o le chiamate telefoniche tramite operatore, senza dover richiedere un ulteriore consenso agli stessi interessati, sempreché non venga esercitato nei confronti del titolare il diritto di opposizione al trattamento (par. 10.7). In pari tempo, nello stesso ambito, l'Autorità ha posto in essere ulteriori azioni di contrasto del *telemarketing* cd. selvaggio e delle offerte promozionali indesiderate, effettuando accertamenti ispettivi ed emettendo ordinanze ingiunzione nei confronti di due importanti società di servizi informatici, specializzate nel settore delle banche dati, condannate al pagamento di rilevanti sanzioni per aver violato provvedimenti prescrittivi già adottati nei loro confronti (par. 10.3).

Sono state altresì prescritte misure a tutela degli interessati in caso di utilizzo, per le attività di *customer care* o *telemarketing*, di *call center* situati in Paesi dove non sono assicurate le garanzie previste dalla normativa comunitaria di protezione dei dati; tra queste, oltre ad una completa informativa, anche l'obbligo per le società che si avvalgono dei *call center*, di darne previa comunicazione al Garante, utilizzando un modello disponibile sul sito web istituzionale, per permettere all'Autorità di valutare la portata del trasferimento dei dati personali al di fuori dall'Unione europea (par. 10.5).

1.7. Il corretto impiego delle informazioni personali per il contrasto delle frodi, entro un quadro normativo chiaro, ha rappresentato un ulteriore delicato ambito di intervento del Garante. Al riguardo sono state formulate osservazioni all'Istituto per la vigilanza sulle assicurazioni (Ivass), in relazione al tema della prevenzione e del contrasto alle frodi nel settore delle assicurazioni Rc auto, in merito alla banca dati dei sinistri e alle neocostituite anagrafe testimoni e anagrafe danneggiati, raccomandando di informare gli interessati, di limitare la consultazione della banca dati ai soli soggetti indicati dalla legge per il solo scopo di rendere più efficace la prevenzione e il contrasto alle frodi assicurative e di limitare a 5 anni il tempo di conservazione dei dati identificativi degli interessati (parti coinvolte nel sinistro, testimoni, *etc.*) (par. 12.2). In materia di frodi nel settore del credito al consumo, con particolare riferimento al furto d'identità, criticità sono state rilevate su uno schema di decreto del Ministero dell'economia e delle finanze preordinato a disciplinare le modalità di funzionamento del sistema pubblico di prevenzione, sul piano amministrativo, istituito presso il Ministero medesimo in relazione al quale, oltre a chiedere il rispetto del principio di finalità e l'adozione di misure di sicurezza adeguate, si è ravvisata la necessità di precisare nel regolamento i diversi livelli di accesso al sistema da parte dei cd. aderenti diretti e indiretti nonché l'opportunità di prevedere modalità di informazione a vantaggio degli interessati delle eventuali incongruenze dei dati riscontrati nelle banche dati pubbliche all'esito delle verifiche effettuate (par. 3.2.2).

Ancora con riferimento ai trattamenti effettuati in ambito privatistico, il Garante (tornando a pronunciarsi su un tema delicato, purtroppo ricorrente nella presente congiuntura economica sfavorevole e già oggetto di un provvedimento generale) ha vietato l'inoltro alla clientela di comunicazioni telefoniche preregistrate senza l'intervento di un operatore per finalità di recupero crediti (par. 12.1).

1.8. Con l'intensificarsi dell'utilizzo di informazioni personali per contrastare il fenomeno tuttora gravissimo dell'evasione fiscale, nonostante le misure di carattere anche legislativo intraprese negli ultimi anni, il Garante ha svolto un'azione decisa

affinché, nell'adempimento degli obblighi di solidarietà, non siano ingiustificatamente lesi diritti fondamentali dei singoli. Per questa ragione, all'esito di un'approfondita verifica preliminare sui trattamenti effettuati dall'Agenzia delle entrate in relazione al cd. redditometro, sono state impartite prescrizioni in ordine ai numerosi profili di criticità rilevati (derivanti, peraltro, anche dallo stesso decreto ministeriale di attuazione del nuovo redditometro), relativi alla qualità ed esattezza dei dati utilizzati dall'Agenzia, all'informativa da rendere al contribuente, all'individuazione in via presuntiva della spesa sostenuta da ciascun contribuente riguardo ad ogni aspetto della vita quotidiana (tempo libero, libri, pasti fuori casa, *etc.*) mediante l'attribuzione alla generalità dei soggetti censiti nell'Anagrafe tributaria della spesa media rilevata dall'Istat (par. 4.7).

1.9. L'impiego dei dati biometrici ha formato oggetto di approfondimenti conoscitivi e di interventi del Garante, sia nell'ambito di verifiche preliminari che a seguito di accertamenti *in loco*: è stato consentito a due banche di dotare i propri promotori finanziari di *tablet* in grado di analizzare i dati biometrici della sottoscrizione apposta dai clienti che desiderano stipulare contratti finanziari in forma elettronica, prescrivendo però contestualmente alle società coinvolte nell'abilitazione e nella gestione dei due sistemi l'adozione di particolari misure a tutela dei dati raccolti e misure volte a garantire comunque ai clienti la possibilità di sottoscrivere i contratti anche attraverso modalità tradizionali (par. 12.5).

1.10. Confermando un indirizzo da tempo seguito dall'Autorità, è stato invece ritenuto sproporzionato l'impiego di dati biometrici per finalità di rilevazione delle presenze, in particolare di insegnanti e personale tecnico-amministrativo in alcuni istituti scolastici (par. 11.2). E proprio nel contesto lavorativo, il numero elevato di segnalazioni pervenute, sovente confermato dagli esiti dei numerosi accertamenti ispettivi disposti dall'Autorità, evidenzia la persistenza di violazioni della disciplina di protezione dei dati personali e della normativa di settore, in particolare in materia di controllo a distanza dei lavoratori (nonostante le semplificazioni procedimentali introdotte, rispetto all'installazione di impianti audiovisivi, dal Ministero del lavoro e delle politiche sociali con circolare del 16 aprile 2012). Se il fenomeno è più marcato in relazione al controllo reso possibile da sistemi di videosorveglianza – rispetto ai quali verifiche a campione sono state effettuate nel 2013 nel settore della grande distribuzione, nel quale il Garante ha talora potuto rilevare la mancanza di licenza prefettizia di guardia particolare giurata in capo al personale della società di vigilanza incaricata di compiti anti-rapina e anti-taccheggio (par. 11.1) –, le segnalazioni si estendono anche a strumenti di controllo meno agevolmente riconoscibili da parte degli interessati (quali la geolocalizzazione o l'analisi della navigazione effettuata tramite i dispositivi di comunicazione elettronica assegnati ai lavoratori), sui quali, peraltro, da tempo il Garante si è espresso con provvedimenti di natura generale.

La grave crisi occupazionale che interessa il Paese determina un sensibile incremento della platea dei candidati alla ricerca di occupazione che, quindi, ricorrono ai più vari canali di intermediazione e, tra questi, a soggetti che, gestendo siti internet (come pur previsto, a determinate condizioni, dalla legge), trattano quantità rilevantissime di dati personali: in questa cornice, meritevole di più ampia considerazione, il Garante – sempre nell'ottica di tutela degli interessati – ha vietato i trattamenti di informazioni relative ad oltre 400 mila aspiranti lavoratori effettuati tramite un sito web per finalità di intermediazione tra domanda ed offerta di lavoro in violazione della disciplina di settore e di protezione dei dati personali (par. 11.3).

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

Anche nel 2013 sono stati approvati numerosi provvedimenti normativi che hanno riflessi sulla materia del trattamento dei dati personali. Fra questi, al fine di offrire una ricognizione, seppur sintetica, tale però da rendere conto dell'eterogeneità delle materie toccate (che rientrano, quindi, nell'area di interesse dell'Autorità), si menzionano:

1) la legge 27 dicembre 2013, n. 147, recante "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge di stabilità 2014)", di cui si riportano di seguito gli aspetti di maggior interesse per l'Autorità:

Legge di stabilità 2014

a) all'art. 3 (Cedolare secca sugli affitti) del d.lgs. 14 marzo 2011, n. 23 (Disposizioni in materia di federalismo fiscale municipale), si inserisce il comma 10-*bis* che, per assicurare il contrasto dell'evasione fiscale nel settore delle locazioni abitative, conferisce ai comuni, in relazione ai contratti di locazione, funzioni di monitoraggio, anche previo utilizzo del registro di anagrafe condominiale (art. 1130, primo comma, n. 6, c.c.); il predetto registro contiene le generalità dei singoli proprietari e dei titolari di diritti reali e di diritti personali di godimento, comprensive del codice fiscale e della residenza o domicilio, i dati catastali di ciascuna unità immobiliare, nonché ogni dato relativo alle condizioni di sicurezza (art. 1, comma 49);
b) nel codice dell'amministrazione digitale (Cad) si inserisce l'art. 62-*ter* (Anagrafe nazionale degli assistiti) che, per rafforzare gli interventi in tema di monitoraggio della spesa del settore sanitario, accelerare il processo di automazione amministrativa e migliorare i servizi per i cittadini e le pp.aa., istituisce nell'ambito del sistema informativo realizzato dal Ministero dell'economia e delle finanze l'Anagrafe nazionale degli assistiti (Ana). Tale Anagrafe, realizzata in accordo con il Ministero della salute in relazione alle specifiche esigenze di monitoraggio dei livelli essenziali di assistenza (lea), subentra, per tutte le finalità previste dalla normativa vigente, alle anagrafi e agli elenchi degli assistiti tenuti dalle singole Asl ai sensi dell'art. 7, l. 7 agosto 1982, n. 526. Entro il 30 giugno 2014, con d.P.C.M., dovranno essere stabiliti, oltre ai contenuti dell'Ana, i criteri per la sua interoperabilità con le altre banche dati di rilevanza nazionale e regionale, il piano per il graduale subentro, le garanzie e le misure di sicurezza da adottare, nonché le modalità di cooperazione della stessa con banche dati già istituite a livello regionale per le medesime finalità, nel rispetto (tra l'altro) della normativa sulla protezione dei dati personali (art. 1, comma 231);
c) a parte il finanziamento garantito dal Ministero dell'economia e delle finanze al Garante, si dispone, seppur con modalità diverse rispetto al passato, il finanziamento incrociato ad opera di altre autorità indipendenti, sostituendo il comma 523 dell'art. 1, l. 24 dicembre 2012, n. 228 (art. 1, comma 416) (ma v. *infra* par. 21.1 con riferimento ai riflessi della sentenza Tar Lazio, Sez. II, depositata il 5 marzo 2014);

d) si prevede che, al fine di conseguire un risparmio di spesa, su proposta del Ministro delle infrastrutture e dei trasporti, con uno o più regolamenti siano adottate misure volte all'unificazione in un unico archivio telematico nazionale dei dati concernenti la proprietà e le caratteristiche tecniche dei veicoli attualmente inseriti nel Pubblico registro automobilistico e nell'archivio nazionale dei veicoli (art. 1, comma 427);

e) un'altra disposizione di interesse riguarda il tetto alle retribuzioni previsto dalle disposizioni di cui all'art. 23-*ter*, d.l. 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla l. 22 dicembre 2011, n. 214, ora applicabile a chiunque riceva a carico delle finanze pubbliche retribuzioni o emolumenti comunque denominati in ragione di rapporti di lavoro subordinato o autonomo intercorrenti con le autorità amministrative indipendenti e con le pp.aa., ivi incluso il personale di diritto pubblico di cui all'art. 3 del testo unico sul pubblico impiego (art. 1, comma 471);

2) il decreto-legge 10 ottobre 2013, n. 114, convertito, con modificazioni, dalla l. 9 dicembre 2013, n. 135, in materia di proroga delle missioni internazionali delle Forze armate e di polizia, che prevede la pubblicità dell'ammontare del trattamento economico e delle spese per vitto, alloggio e viaggi del personale in missione, al fine di garantire la trasparenza di tali operazioni, nel rispetto della vigente legislazione in materia di protezione dei dati (art. 5, comma 6). In occasione della sua adozione è stato altresì approvato un ordine del giorno che impegna il Governo a disporre l'avvio della raccolta dei dati sensibili riconducibili alle manifestazioni della sindrome da stress post-traumatico da combattimento, anche allo scopo di predisporre a vantaggio degli interessati le misure di sostegno e riabilitazione necessarie (9/1670-A-R/88 Buonanno, Molteni, Fedriga);

Sistema nazionale delle anagrafi degli studenti

3) il decreto-legge 12 settembre 2013, n. 104, convertito, con modificazioni, dalla l. 8 novembre 2013, n. 128, in materia di misure urgenti in materia di istruzione, università e ricerca, il quale prevede che le anagrafi regionali degli studenti e l'anagrafe nazionale degli studenti siano integrate nel sistema nazionale delle anagrafi degli studenti del sistema educativo di istruzione e di formazione (art. 13). Le modalità di integrazione e di accesso alle anagrafi saranno definite, prevedendo la funzione di coordinamento del Miur, nel rispetto delle disposizioni dell'art. 3, comma 4, d.lgs. 15 aprile 2005, n. 76, previo parere del Garante. È altresì previsto che, per l'erogazione dei servizi di propria competenza, gli enti locali possano accedere ai dati delle anagrafi degli studenti nel rispetto della normativa sulla protezione dei dati personali. Infine, per una migliore integrazione scolastica degli alunni disabili mediante l'assegnazione del personale docente di sostegno, le istituzioni scolastiche sono autorizzate a trasmettere per via telematica alla banca dati dell'anagrafe nazionale degli studenti le diagnosi funzionali degli alunni interessati prive di elementi identificativi (art. 12, comma 5, l. n. 104/1992). Apposito decreto del Miur dovrà definire, previo parere del Garante, i criteri e le modalità concernenti la possibilità di accesso ai dati sensibili nonché la sicurezza dei medesimi, assicurando nell'ambito dell'anagrafe nazionale degli studenti, la separazione tra la partizione contenente le diagnosi funzionali e gli altri dati;

Sistema statistico nazionale

4) il decreto-legge 31 agosto 2013, n. 101, convertito, con modificazioni, dalla l. 30 ottobre 2013, n. 125, recante disposizioni urgenti per il perseguimento di obiettivi di razionalizzazione nelle pp.aa., del quale si segnalano in particolare due disposizioni:

a) l'art. 8-*bis* (Disposizioni riguardanti l'Istituto nazionale di statistica e il Sistema statistico nazionale), frutto di un emendamento del Governo, che apporta importanti modifiche al d.lgs. 6 settembre 1989, n. 322 (recante norme sul Sistema statistico nazionale). In primo luogo, si abroga

il comma 2 dell'art. 6-*bis* (Trattamenti di dati personali), il quale prevedeva che nel Programma statistico nazionale (Psn) fossero illustrate le finalità perseguite e le garanzie previste dal decreto medesimo e dalla l. 31 dicembre 1996, n. 675. Al contempo, il comma in questione stabiliva che il programma (adottato sentito il Garante) indicasse anche i dati di cui agli artt. 22 e 24 della medesima legge, le rilevazioni per le quali i dati sono trattati e le modalità di trattamento (art. 8-*bis*, comma 1, lett. *a*). Con riferimento al Psn annualmente aggiornato, si prevedono, altresì, modalità di raccordo e di coordinamento con i programmi statistici predisposti a livello regionale e si individuano "le varianti che possono essere diffuse in forma disaggregata, ove ciò risulti necessario per soddisfare particolari esigenze conoscitive anche di carattere internazionale o europeo" (art. 8-*bis*, comma 1, lett. *c*), nn. 1 e 2);

b) l'art. 11 sulla semplificazione e razionalizzazione del sistema di controllo della tracciabilità dei rifiuti (Sistri) e in materia di energia, il quale modifica, tra l'altro, l'art. 188-*bis* (Controllo della tracciabilità dei rifiuti) del d.lgs. 3 aprile 2006, n. 152, recante norme in materia ambientale, introducendo il comma 4-*bis* (comma 7). Al riguardo si prevede che, con decreto del Ministro dell'ambiente e della tutela del territorio e del mare, si proceda periodicamente alla semplificazione e all'ottimizzazione del Sistri sulla base dell'evoluzione tecnologica. La norma è finalizzata, tra l'altro, "ad assicurare un'efficace tracciabilità dei rifiuti e a ridurre i costi di esercizio del sistema, anche mediante integrazioni con altri sistemi che trattano dati di logistica e mobilità delle merci e delle persone [...] e ad assicurare la modifica, la sostituzione o l'evoluzione degli apparati tecnologici, anche con riferimento ai dispositivi periferici per la misura e certificazione dei dati". Inoltre, anche al fine della riduzione dei costi, il Ministero dell'ambiente e della tutela del territorio e del mare, previo parere del Garante, può autorizzare il concessionario del sistema informativo a "rendere disponibile l'informazione territoriale, nell'ambito della integrazione dei sistemi informativi pubblici, a favore di altri enti pubblici o società interamente a capitale pubblico [...] anche al fine di fornire servizi aggiuntivi agli utenti. Sono comunque assicurate la sicurezza e l'integrità dei dati di tracciabilità";

Controllo della tracciabilità dei rifiuti (Sistri)

5) il decreto-legge 14 agosto 2013, n. 93, convertito, con modificazioni, dalla l. 15 ottobre 2013, n. 119, recante disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle Province. Le seguenti disposizioni sono di particolare interesse:

Violenza sessuale e di genere

a) l'art. 3, nel disporre misure di prevenzione per condotte di violenza domestica, prevede la possibilità per il questore di procedere all'ammonimento dell'autore di un fatto riconducibile al reato di cui all'art. 582, comma 2, c.p. (Lesione personale) nell'ambito di violenza domestica, anche in assenza di querela (comma 1); ad ogni modo, relativamente agli atti del procedimento per l'adozione dell'ammonimento dovranno essere omesse le generalità dell'eventuale segnalante (comma 4). Inoltre, si prevede che il Ministero dell'interno elabori annualmente un'analisi criminologica della violenza di genere, anche attraverso i dati contenuti nel Centro elaborazione dati interforze del Dipartimento della pubblica sicurezza. Tale analisi costituisce un'autonoma sezione della relazione annuale al Parlamento prevista dall'art. 113, l. n. 121/1981 (comma 3);

b) l'art. 5 è volto a promuovere un piano d'azione straordinario contro la violenza sessuale e di genere tra le cui finalità si prevede, tra l'altro, un raffor-

zamento della collaborazione tra le istituzioni coinvolte, nonché una raccolta strutturata dei dati del fenomeno anche attraverso il coordinamento di banche dati già esistenti;

Frode informatica

c) l'art. 9 modifica le norme sul reato di frode informatica (art. 640-*ter* c.p.), prevedendo un incremento di pena quando il reato sia commesso con indebito utilizzo dell'identità digitale (comma 1). Inoltre, con la medesima disposizione si sarebbe dovuto modificare l'art. 24-*bis*, d.lgs. 8 giugno 2001, n. 231 (Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della l. 29 settembre 2000, n. 300), estendendo la sanzione prevista per i delitti informatici e per il trattamento illecito di dati (sanzione pecuniaria da cento a cinquecento quote) anche ai delitti previsti dalla Parte III, Titolo III, Capo II del Codice in materia di protezione dei dati personali; la disposizione è stata poi soppressa in fase di conversione del decreto;

Sistema antifrode contro il furto di identità

d) il medesimo art. 9, al comma 3, apporta modifiche al d.lgs. 13 agosto 2010, n. 141, recante l'attuazione della direttiva 2008/48/CE relativa ai contratti di credito ai consumatori. In particolare, è inserito il comma 7-*bis* all'art. 30-*ter* relativo all'istituzione di un sistema pubblico di prevenzione delle frodi nel settore del credito al consumo e dei pagamenti dilazionati o differiti, con specifico riferimento al furto di identità. Si prevede, al riguardo, che gli aderenti (cioè le banche e gli altri soggetti che partecipano al sistema antifrode), nell'ambito della propria specifica attività, possano inviare all'ente gestore del sistema, istituito presso il Ministero dell'economia e delle finanze, richieste di verifica dell'autenticità dei dati contenuti nella documentazione fornita dalle persone fisiche nei casi in cui ritengono utile, sulla base della valutazione degli elementi acquisiti, accertarne l'identità. Con tale norma si amplia il novero dei documenti oggetto di possibile riscontro per controllarne la autenticità e la riconducibilità al legittimo titolare, al di là delle ipotesi già indicate dal decreto legislativo e dal relativo regolamento di attuazione in fase di adozione da parte del predetto Ministero. La modifica in questione, tuttavia, era stata già introdotta dal legislatore in sede di conversione del d.l. 21 giugno 2013, n. 69, recante disposizioni urgenti per il rilancio dell'economia, con l'art. 16-*bis* (Modifiche al d.lgs. 13 agosto 2010, n. 141, in materia di accesso alle banche dati pubbliche);

Obblighi in tema di trasparenza

e) in tema di protezione civile, l'art. 10 modifica il d.lgs. 14 marzo 2013, n. 33, recante il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, aggiungendo il comma 1-*bis* all'art. 42 (Obblighi di pubblicazione concernenti gli interventi straordinari e di emergenza che comportano deroghe alla legislazione vigente). Il nuovo comma prevede che i commissari delegati di cui dall'art. 5, comma 4, della l. 24 febbraio 1992, n. 225, svolgano direttamente le funzioni di responsabili per la prevenzione della corruzione di cui all'art. 1, comma 7, della l. 6 novembre 2012, n. 190 e le funzioni di responsabili per la trasparenza di cui all'art. 43, d.lgs. n. 33/2013;

Beni culturali

6) il decreto-legge 8 agosto 2013, n. 91, convertito, con modificazioni, dalla l. 7 ottobre 2013, n. 112, recante disposizioni urgenti per la tutela, la valorizzazione e il rilancio dei beni e delle attività culturali e del turismo, in base al quale, al fine di ottimizzare le risorse disponibili e di facilitare il reperimento e l'uso dell'informazione culturale e scientifica, il Ministero dei beni e delle attività culturali e del turi-

smo ed il Ministero dell'istruzione, dell'università e della ricerca adottano strategie coordinate per l'unificazione delle banche dati rispettivamente gestite, quali quelle riguardanti l'Anagrafe nazionale della ricerca, il deposito legale dei documenti digitali e la documentazione bibliografica (art. 4);

Legge europea e Legge di delegazione europea

7) la legge 6 agosto 2013, n. 97 recante disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2013, che prevede disposizioni di attuazione di norme europee. In particolare:

a) l'art. 9 reca disposizioni in materia di monitoraggio fiscale (Caso EU Pilot 1711/11/TAXU), modificando il d.l. 28 giugno 1990, n. 167, convertito, con modificazioni, dalla l. 4 agosto 1990, n. 227;
b) l'art. 28, reca modifiche al d.lgs. 10 agosto 2007, n. 162, in materia di indagini sugli incidenti ferroviari (Caso EU Pilot 1254/10/MOVE);
c) l'art. 31 reca attuazione della decisione 2009/750/CE della Commissione sulla definizione del servizio europeo di telepedaggio e dei relativi elementi tecnici (Caso EU Pilot 4176/12/MOVE);

8) la legge 6 agosto 2013, n. 96, recante la delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2013. La legge prevede l'attuazione di diverse direttive, alcune delle quali d'interesse sotto il profilo della protezione dei dati personali (contenenti apposite clausole di salvaguardia della normativa e delle garanzie per la protezione dei dati personali degli utenti), quali le direttive: 2011/16/EU sulla cooperazione amministrativa nel settore fiscale; 2011/24/EU concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera; 2011/82/UE sullo scambio transfrontaliero di informazioni sulle infrazioni in materia di sicurezza stradale (con riguardo alla quale l'Autorità ha partecipato ad un tavolo di lavoro presso l'ufficio legislativo del Ministro degli affari europei in relazione alla stesura dello schema di decreto legislativo attuativo e quindi reso il parere del 9 gennaio 2014, n. 2, doc. web n. 2904320);

Banca dati delle politiche attive e passive

9) il decreto-legge 28 giugno 2013, n. 76, convertito dalla l. 9 agosto 2013, n. 99, recante primi interventi urgenti per la promozione dell'occupazione, in special modo giovanile, e della coesione sociale. In particolare, l'art. 8 istituisce la banca dati delle politiche attive e passive all'interno delle strutture del Ministero del lavoro e delle politiche sociali, destinata a raccogliere le informazioni sui soggetti da collocare nel mondo del lavoro, sui servizi erogati a tal fine e sulle opportunità di impiego. Essa è costituita con il contributo informativo delle regioni e delle province autonome, delle province, dell'Isfol, dell'Istituto nazionale di previdenza sociale, di Italia Lavoro s.p.a., del Ministero dell'istruzione, dell'università e della ricerca, del Ministero dell'interno, del Ministero dello sviluppo economico, delle Università pubbliche e private e delle Camere di commercio, industria, artigianato e agricoltura. La banca dati costituisce una componente del Sistema informativo lavoro (Sil) *ex* art. 11, d.lgs. n. 469/1997 e della Borsa continua nazionale del lavoro *ex* art. 15, d.lgs. n. 276/2003. Nella nuova banca dati confluiscono una serie di banche dati già esistenti (quali la banca dati percettori *ex* art. 19, comma 4, d.l. n. 185/2008 convertito con la l. n. 2/2009, l'anagrafe nazionale degli studenti e dei laureati delle università *ex* art. 1-*bis*, d.l. n. 105/2003 convertito con l. n. 170/2003) e la dorsale informativa *ex* art. 4, comma 51, l. n. 92/2012. Il Ministero del lavoro e delle politiche sociali è autorizzato a stipulare convenzioni con soggetti pubblici e privati per far confluire i dati nella banca dati in questione (ed eventualmente in altre banche dati costituite con la stessa finalità) nonché per determinare le modalità più opportune di raccolta ed elaborazione dei dati su domanda e offerta di lavoro secondo le migliori tecniche ed esperienze (comma 5);

Prevenzione e la lotta contro la violenza nei confronti delle donne

10) la legge 27 giugno 2013, n. 77, recante la ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica, fatta a Istanbul l'11 maggio 2011. Nel corso dei lavori parlamentari, l'Autorità ha segnalato all'ufficio legislativo del Ministero degli affari esteri l'opportunità di integrare il disegno di legge sotto il profilo della protezione dei dati personali in relazione all'art. 11, par. 1, lett. *a*), della Convenzione, nella parte in cui prevede la raccolta di "dati statistici disaggregati" su questioni relative a qualsiasi forma di violenza che rientri nel campo di applicazione della Convenzione (nota 21 maggio 2013). La disposizione appare, infatti, in conflitto con la normativa nazionale in materia di rilevazioni statistiche (d.lgs. 6 settembre 1989, n. 322) e con le norme contenute nel Codice e rischia di arrecare pregiudizio alla riservatezza e alla dignità delle persone coinvolte in fatti di violenza sulle donne e, in *primis*, alle vittime stesse. Ciò in quanto la disposizione autorizza – in via generale e senza alcuna necessità di valutazione e ponderazione al riguardo – il trattamento di dati personali anche in forma disaggregata e non, invece, anonima o comunque "aggregata" come prevede la normativa sopra citata al fine di evitare l'identificabilità degli interessati. Infatti, l'art. 9, d.lgs. n. 322/1989 – cui rinvia l'art. 108 del Codice – stabilisce che i dati raccolti nell'ambito di rilevazioni statistiche comprese nel Psn da parte degli uffici di statistica non possano essere esternati, comunicati o diffusi se non in forma aggregata in modo che non se ne possa trarre alcun riferimento a persone identificabili. Al riguardo, si segnala che il predetto disegno di legge non è stato integrato come richiesto dall'Autorità;

Rilancio dell'economia

11) il decreto-legge 21 giugno 2013, n. 69, convertito dalla l. 9 agosto 2013, n. 98, recante disposizioni urgenti per il rilancio dell'economia, recante diverse disposizioni di interesse per l'Autorità, in relazione ad alcune delle quali il Garante ha anche segnalato al Parlamento e al Governo specifiche criticità (cfr. note 5 luglio 2013, richiamate nel comunicato stampa del 9 luglio 2013, doc. web n. 2522062), ed in particolare:

Liberalizzazione dell'accesso ad internet "senza fili"

a) l'art. 10 del decreto-legge, nella versione finale approvata dal Parlamento, "liberalizza" l'offerta di accesso alla rete Internet tramite tecnologia *WiFi* sotto tre aspetti: non è richiesta l'identificazione personale degli utilizzatori; quando l'offerta di accesso ad internet non costituisce l'attività commerciale prevalente del gestore (quali bar, alberghi, altri esercizi commerciali aperti al pubblico, università, *etc.*), non sono richieste né la licenza del questore (art. 7, d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, dalla l. 31 luglio 2005, n. 155), né l'autorizzazione ministeriale *ex* art. 25 del d.lgs. 1° agosto 2003, n. 259; si facilita, infine, l'installazione delle relative apparecchiature (abrogazione del cd. patentino installatori, cioè dell'obbligo di affidare i lavori di allacciamento dei terminali a imprese abilitate). Il testo approvato definitivamente è il frutto di interventi modificativi che si sono succeduti nel corso dei lavori parlamentari. L'originaria versione dell'art. 10 presentava invece forti criticità che il Garante ha segnalato al Parlamento e al Governo. La disposizione originaria obbligava infatti i gestori a "garantire la tracciabilità del collegamento (MAC *address*)" e stabiliva che la "registrazione della traccia delle sessioni", ove non associata all'identità dell'utilizzatore, non costituiva trattamento di dati personali e non richiedeva adempimenti giuridici (commi 1, secondo periodo e 2, primo periodo). Il Garante ha osservato (nota 5 luglio 2013) preliminarmente che con tali previsioni il Governo – probabilmente quale misura "compensativa" sotto il profilo della sicurezza e dell'ordine pubblico rispetto al venir meno della previa identificazione della persona che accede

ad internet – avrebbe di fatto (re)introdotto l'obbligo per i "gestori" di tracciare (o comunque garantire la tracciabilità di) alcune informazioni che, per quanto non individuate in maniera chiara, sono comunque "riconducibili" all'accesso alla rete da parte dell'utilizzatore del terminale. Occorre infatti ricordare che taluni obblighi di monitoraggio e registrazione di dati erano stati stabiliti dal d.l. n. 144/2005 (cd. decreto Pisanu) per categorie di "gestori" diversi da coloro che offrono accesso a internet con tecnologia *WiFi*, e sono stati successivamente soppressi anche in ragione delle difficoltà e degli oneri legati alla loro applicazione (d.l. n. 225/2010). L'Autorità ha sottolineato che tali disposizioni, nell'escludere che il trattamento in parola costituisse un trattamento di dati personali, rischiavano di "impattare" sulla tutela dei diritti fondamentali e di confliggere con la definizione stessa di dato personale contenuta, oltre che nel Codice, nella stessa direttiva 95/46/CE. Quest'ultima, infatti, contiene una definizione di "dato personale" molto ampia, che ricomprende "qualunque informazione concernente una persona fisica identificata o identificabile [...] direttamente o indirettamente, in particolare mediante riferimento a un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità" (art. 2, par. 1, lett. *a*), direttiva 95/46/CE). In tale quadro, l'Autorità, consapevole dell'importanza dell'esigenza di contemperare la liberalizzazione dell'accesso a internet con la tutela della sicurezza pubblica e il contrasto della criminalità, ha ritenuto che fosse opportuno "stralciare" la disposizione dal decreto-legge ritenendo che tali problematiche, con le connesse implicazioni per la protezione dei dati personali, avrebbero potuto, semmai, trovare un più meditato approfondimento in una sede diversa e più idonea di quella consentita dai ristretti tempi di approvazione di un provvedimento d'urgenza;

b) l'art. 17 dispone misure per favorire la realizzazione del Fascicolo sanitario elettronico (*infra* Fse) modificando l'art. 12 (Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario) del d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221. Anche l'art. 17 presentava (e presenta tuttora, nella versione definitivamente approvata) criticità sotto il profilo della protezione dei dati personali che il Garante ha segnalato, in particolare al Ministro della salute. L'art. 12 nella sua formulazione originaria, prevedeva che – ferma restando la libera espressione del consenso dell'assistito ai fini dell'alimentazione del Fse – le Regioni e le Province autonome, il Ministero del lavoro e delle politiche sociali e il Ministero della salute potessero perseguire le finalità di studio e ricerca scientifica, nonché di programmazione sanitaria e monitoraggio loro assegnate "senza l'utilizzo dei dati identificativi degli assistiti e dei documenti clinici presenti nel Fse". Ciò sul presupposto che per tali finalità, le quali non attengono alla cura della persona, fosse sufficiente utilizzare informazioni non identificative dei pazienti, in applicazione dei principi di necessità, proporzionalità e indispensabilità nel trattamento dei dati personali, e senza che fossero in alcun modo presi in considerazione documenti clinici. Con la modifica operata dal decreto-legge (art. 17, comma 1, lett. *b*) i predetti soggetti pubblici sono, invece, autorizzati a utilizzare anche i "documenti clinici". Il Garante ha espresso forti perplessità su tale ampliamento del novero delle informazioni oggetto di trattamento per finalità diverse da quelle di cura. Per effetto della modifica normativa, infatti, potrebbe essere trattata dalle

Fascicolo sanitario elettronico

Regioni, dalle Province autonome e dai Ministeri un'enorme mole di dati personali sensibili (si pensi alle risultanze diagnostiche radiologiche, o a quelle di analisi cliniche, *etc.*), che rappresenta un patrimonio informativo prezioso per gli operatori sanitari nel momento in cui devono fare una diagnosi o prestare le cure mediche, ma sproporzionato per lo svolgimento di attività quali quelle di ricerca scientifica o programmazione sanitaria. Il Garante ha perciò segnalato la necessità di una modifica della norma in modo da assicurare ai predetti soggetti pubblici un utilizzo selettivo delle sole informazioni veramente utili e pertinenti per il perseguimento delle finalità loro assegnate, suggerendo di integrare l'art. 12 con la previsione che il regolamento di attuazione di tale disciplina (art. 12, comma 7, d.l. n. 179/2012) – al quale è demandato di definire, fra l'altro, i contenuti del Fse – individuasse espressamente anche i "documenti sanitari" utilizzabili per tali finalità "amministrative". Questa osservazione non è stata, purtroppo, recepita dal Parlamento. L'Autorità potrà in ogni caso confermare le proprie perplessità e fornire le conseguenti indicazioni in occasione del parere da rendere sullo schema di decreto di attuazione dell'art. 12, il quale dovrà comunque individuare i "contenuti del Fse" e i "livelli diversificati di accesso". Al Senato il Governo ha accolto un ordine del giorno presentato dalla senatrice Spilabotte (G84.401-testo 2) con cui si impegna a "valutare l'opportunità dell'adozione, al fine di garantire la *privacy* dei cittadini, di apposite misure che prevedano la possibilità di consultazione del Fse per le finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico e di programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria, escludendo l'utilizzo, da parte dei soggetti incaricati alla consultazione, dei dati identificativi degli assistiti e dei documenti clinici presenti nel Fse". L'art. 17 (e, conseguentemente, l'art. 12 del d.l. n. 179/2012) ha subito più modifiche nel corso dei lavori parlamentari. Si sono introdotti nuovi termini, stabilendo che le regioni e le province autonome, per provvedere all'istituzione del Fse, entro il 30 giugno 2014 devono presentare all'Agenzia per l'Italia Digitale (AgID) al Ministero della salute i piani di progetto per la sua realizzazione. È altresì previsto che tali piani siano redatti in base a linee guida predisposte, entro il 31 marzo 2014, dall'AgID e dal Ministero della salute, anche mediante l'ausilio di enti pubblici di ricerca. A seguito degli emendamenti approvati al Senato, anche in base ai piani di progetto presentati dalle Regioni, l'AgID cura, in accordo con il Ministero della salute, con le Regioni e le Province autonome, la progettazione e la realizzazione dell'"infrastruttura nazionale" necessaria a garantire l'interoperabilità dei fascicoli regionali (art. 12, comma 15-*ter*). Le Regioni possono partecipare alla definizione, realizzazione ed utilizzo di tale infrastruttura nazionale, conforme ai criteri stabiliti dal decreto di cui al comma 7, resa disponibile dall'AgID, che dovrà essere allestita entro il 31 dicembre 2015 (nuovo comma 15). Di particolare importanza è la nuova previsione di un "*dossier* farmaceutico" (aggiornato da parte della farmacia che provvede alla somministrazione del medicinale), quale parte integrante del Fse. In merito, è stato introdotto il comma 2-*bis* dell'art. 12 in base al quale, "per favorire la qualità, il monitoraggio, l'appropriatezza nella dispensazione dei medicinali e l'aderenza alla terapia ai fini della sicurezza del paziente, è istituito il *dossier* farmaceutico quale parte specifica del Fse, aggiornato a cura della farmacia che

effettua la dispensazione". I contenuti del *dossier* saranno individuati dal decreto attuativo di cui al comma 7. Infine, quale ultima novità rispetto all'originaria versione dell'articolo in parola, si segnala che l'approvazione dei piani di progetto da parte dell'Agenzia Digitale e del Ministero della salute potrà essere condizionata alla "piena fruibilità dei dati regionali a livello nazionale, per indagini epidemiologiche, valutazioni statistiche, registri nazionali e raccolta dati a fini di programmazione sanitaria nazionale" (comma 15-*quater*, lett. *a*);

c) nella segnalazione al Parlamento del 5 luglio il Garante ha espresso la propria contrarietà alla possibile riproposizione di disposizioni volte ad escludere dall'applicazione del Codice gli imprenditori individuali, all'epoca contenute in una bozza di disegno di legge in materia di semplificazioni poi successivamente presentato dal Governo (AS 958, all'esame della Commissione affari costituzionali del Senato). La proposta di legge (art. 17 - Semplificazioni in materia di *privacy*) stabilisce che "ai fini dell'applicazione del [...] Codice l'imprenditore è considerato persona giuridica relativamente ai dati concernenti l'esercizio dell'attività d'impresa". L'Autorità ha ribadito le perplessità – già manifestate peraltro in occasione della presentazione al Parlamento della Relazione 2012 – circa l'introduzione di una norma che, sostanzialmente, finirebbe con il privare le persone fisiche – sia pure quando agiscano nell'esercizio della propria attività imprenditoriale – del diritto alla protezione dei dati personali, in contrasto con la direttiva 95/46/CE. La norma rischia, peraltro, di sortire effetti paradossali e – in contrasto con le finalità perseguite – pregiudizievoli per la stessa attività d'impresa del piccolo imprenditore, stante la difficoltà di distinguere, in concreto, il dato della persona fisica da quello riferito alla sua qualità di imprenditore individuale. Così potrebbe accadere, ad esempio, che, in caso di mancato o ritardato pagamento di rate per l'acquisto di beni di consumo, il soggetto venga inserito in una centrale rischi e in conseguenza di ciò si veda negare il credito per l'attività di impresa, con il conseguente rischio di estromissione dal mercato. Mentre oggi tale individuo può rivolgersi al Garante per esercitare il diritto d'accesso e, se del caso, gli altri diritti previsti dall'art. 7 del Codice, ove la norma venisse approvata, lo stesso sarebbe privato di tale tutela.

Imprese individuali

Sotto altro profilo, il Garante ha espresso perplessità anche di ordine metodologico. Ove le norme fossero approvate, si realizzerebbe una significativa modifica a parti determinanti della disciplina in materia di protezione dei dati personali, peraltro a breve distanza dalle novelle che hanno già ridotto, in misura rilevante, la categoria dei soggetti di diritto cui si applicano le garanzie del Codice. Le continue modifiche agli istituti fondativi della disciplina della protezione dei dati – apportate, peraltro, anche con decreto-legge e al di fuori da un progetto organico di riforma – rischiano inoltre di ingenerare difficoltà applicative e dubbi interpretativi idonei a vanificare le stesse (auspicate) finalità di semplificazione;

d) l'art. 14, comma 1, aggiungendo il comma 3-*quater* all'art. 10, d.l. 13 maggio 2011, n. 70, convertito, con modificazioni, dalla l. 12 luglio 2011, n. 106, nella versione originaria consentiva al cittadino di richiedere una casella di Pec, nonché di indicare la stessa quale proprio domicilio digitale all'atto della richiesta del "documento unificato" secondo le modalità stabilite con decreto del Ministro dell'interno. In sostanza con tale disposizione si dava la possibilità al cittadino di presentare la richiesta di attribu-

Domicilio digitale

zione di un indirizzo Pec da far valere quale domicilio digitale (istituito ai sensi dell'art. 3-*bis*, d.lgs. 7 marzo 2005, n. 82 (Cad) in occasione della richiesta di rilascio del documento digitale unificato (ddu), ancora in corso di attuazione e destinato a integrare in un unico documento la carta d'identità elettronica e la tessera sanitaria. Con una modifica approvata dalla Camera dei deputati, si è precisato che l'assegnazione al cittadino di una casella di Pec con la funzione di domicilio digitale, attivabile in modalità telematica dall'interessato, possa avvenire oltre che all'atto della richiesta del documento unificato, anche all'atto dell'iscrizione anagrafica o della dichiarazione di cambio di residenza a partire dall'entrata a regime dell'Anagrafe nazionale della popolazione residente, di cui all'art. 2, d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221. Con una ulteriore modifica approvata alla Camera, al medesimo art. 10, d.l. n. 70/2011, è stato aggiunto un altro comma (3-*quinquies*), il quale stabilisce che il predetto documento unificato (ddu) sostituisce, a tutti gli effetti di legge, il tesserino di codice fiscale rilasciato dall'Agenzia delle entrate. Inoltre, con l'art. 14, comma 1-*bis*, aggiunto al decreto-legge con emendamento approvato al Senato, si modifica l'art. 47, comma 2, lett. *c*), del Cad sulla trasmissione dei documenti attraverso la posta elettronica tra le pp.aa., precisando che è comunque esclusa la trasmissione di documenti a mezzo fax ai fini della verifica della provenienza delle comunicazioni. Conseguentemente, con l'art. 14, comma 1-*ter*, anch'esso aggiunto al Senato, si sostituisce l'art. 42 (Accertamenti d'ufficio), comma 3, d.P.R. n. 445/2000, recante il testo unico in materia di documentazione amministrativa, precisando che l'amministrazione procedente opera l'acquisizione d'ufficio esclusivamente per via telematica;

Sistema pubblico di identità digitale (Spid)

e) l'art. 17-*ter*, introdotto nel corso dei lavori alla Camera, modifica l'art. 64 del Cad prevedendo la costituzione, a cura dell'Agenzia per l'Italia Digitale, del Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (*infra* Spid), al fine di favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese (nuovo comma 2-*bis* dell'art. 64 del Cad). Conseguentemente, il nuovo comma 2 del medesimo art. 64 del Cad prevede ora che le pp.aa. possano consentire l'accesso in rete ai propri servizi solo mediante gli strumenti già previsti al comma 1 (cioè carta d'identità elettronica e Cns), ovvero mediante servizi offerti, appunto, dal sistema Spid. Quest'ultimo è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia Digitale, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pp.aa., in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati (nuovo comma 2-*ter* dell'art. 64 del Cad).

Con d.P.C.M., su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, sentito il Garante, saranno definite le caratteristiche del sistema Spid, anche con riferimento al modello architetturale e organizzativo del sistema, alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale, agli *standard* tecnologici e alle soluzioni tecniche e organizzative da adottare al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese (nuovo comma 2-*sexies* dell'art. 64 del Cad);

f) l'art. 34 reca disposizioni in materia di trasmissione in via telematica di alcuni certificati medici (certificato medico di gravidanza indicante la data presunta del parto, certificato di parto, certificato di interruzione di gravidanza) mediante la modifica dell'art. 21, d.lgs. 26 marzo 2001, n. 151, recante il testo unico delle disposizioni legislative in materia di tutela e sostegno della maternità e della paternità. In particolare, con disposizioni che troveranno applicazione solo dal novantesimo giorno successivo alla data di entrata in vigore del previsto decreto di attuazione, si stabilisce che la trasmissione del certificato medico di gravidanza indicante la data presunta del parto all'Inps avvenga esclusivamente per via telematica direttamente dal medico del Servizio sanitario nazionale (o con esso convenzionato); al riguardo, saranno adottate le modalità e si utilizzeranno i servizi definiti con decreto dei Ministri del lavoro e delle politiche sociali e della salute, prevedendo comunque l'utilizzo del sistema di trasmissione delle certificazioni di malattia di cui al decreto del Ministro della salute 26 febbraio 2010 (art. 21, comma 1-*bis*, d.lgs. n. 151/2001). Si prevede poi che la trasmissione all'Inps del certificato di parto o del certificato di interruzione di gravidanza debba essere effettuata esclusivamente per via telematica dalla competente struttura sanitaria pubblica o privata convenzionata con il Servizio sanitario nazionale, secondo le modalità e utilizzando i servizi definiti con il suddetto decreto interministeriale (art. 21, comma 2-*bis*);

Trasmissione dei certificati medici

g) l'art. 43 (Disposizioni in materia di trapianto) modifica il secondo comma dell'art. 3 del regio decreto 18 giugno 1931, n. 773 (concernente il rilascio della carta d'identità), prevedendo che i comuni trasmettano i dati relativi al consenso o al diniego alla donazione degli organi – cha già oggi ricevono al momento della richiesta di rilascio del documento d'identità – al sistema informativo trapianti, di cui all'art. 7, comma 2, l. 1° aprile 1999, n. 91. Con un emendamento approvato alla Camera dei deputati, il citato art. 43 è stato integrato con un nuovo comma (1-*bis*) in base al quale il consenso o il diniego alla donazione degli organi confluiscono nel Fse;

Donazione di organi

12) il decreto-legge 8 aprile 2013, n. 35, convertito dalla l. 6 giugno 2013, n. 64, recante disposizioni urgenti per il pagamento dei debiti scaduti della p.a., in base al quale sono esclusi dal vincolo del patto di stabilità interno una serie di pagamenti sostenuti dagli enti locali, previa comunicazione, mediante sito web della Ragioneria, degli spazi finanziari necessari per sostenere i pagamenti (art. 1, commi 1 e 2). Qualora i responsabili dei servizi interessati non abbiano richiesto senza giustificato motivo gli spazi finanziari ovvero non abbiano effettuato entro il 2013 pagamenti per almeno il 90 % degli spazi concessi, la procura regionale competente della Corte dei conti esercita l'azione nei confronti degli stessi, su segnalazione del collegio dei revisori dei singoli enti locali. Al riguardo, si segnala che le sentenze di condanna emesse dalla Corte dei conti avverso i predetti soggetti restano pubblicate sul sito istituzionale dell'ente fino a quando non siano state eseguite per l'intero importo, facendo salve le cautele previste dalla normativa in materia di tutela dei dati personali (art. 1, comma 4).

Obblighi in tema di trasparenza

Si segnala, inoltre, che "i piani dei pagamenti [...] sono pubblicati dall'ente nel proprio sito internet per importi aggregati per classi di debiti", in conformità all'art. 18 (Amministrazione aperta) del d.l. 22 giugno 2012, n. 83, convertito, con modificazioni, dalla l. 7 agosto 2012, n. 174, concernente la pubblicazione di informazioni sul sito internet delle pp.aa. (norma nel frattempo abrogata dall'art. 53, d.lgs. 14 marzo 2013, n. 33, in materia di trasparenza) (art. 6, comma 3). L'art. 6, comma 11, prevede, inoltre, che i decreti e provvedimenti previsti dal Capo I siano pubbli-

cari nella sezione «Amministrazione trasparente» dei siti internet delle amministrazioni competenti, con le modalità individuate dal menzionato d.lgs. n. 33/2013. Infine, l'art. 7 reca disposizioni in materia di ricognizione dei debiti contratti dalle pp.aa. e, al comma 4, prevede l'obbligo per le pp.aa. debitrici di comunicare l'elenco completo dei debiti non estinti, con l'indicazione dei dati identificativi del creditore nonché i dati del pagamento, garantendo l'aggiornamento dello stato dei debiti mediante un'apposita piattaforma elettronica per la gestione telematica del rilascio delle certificazioni delle somme dovute;

Trasmissione di dati sanitari

13) il decreto-legge 25 marzo 2013, n. 24, recante disposizioni urgenti in materia sanitaria, convertito dalla l. 23 maggio 2013, n. 57. Il provvedimento presenta una norma di interesse, in base alla quale le strutture sanitarie che hanno in cura pazienti con medicinali per terapie avanzate a base di cellule staminali mesenchimali, devono trasmettere a determinati organismi "informazioni dettagliate sulle indicazioni terapeutiche per le quali è stato avviato il trattamento, sullo stato di salute dei pazienti e su ogni altro elemento utile alla valutazione degli esiti e degli eventi avversi, con modalità tali da garantire la riservatezza dell'identità dei pazienti" (art. 2, comma 4). La disposizione normativa in questione è stata significativamente modificata e integrata nel corso dell'esame parlamentare, in particolare ampliando sia la platea delle strutture sanitarie tenute a trasmettere i dati, sia quella dei soggetti cui i dati devono essere resi disponibili.

2.1.2. I decreti legislativi

Quanto alla normativa primaria delegata, particolarmente importante è il decreto legislativo 14 marzo 2013, n. 33, recante il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pp.aa. (adottato ai sensi dell'art. 1, commi 35 e 36, l. 6 novembre 2012, n. 190), per l'impatto che esso ha avuto sull'applicazione della normativa in materia di protezione dei dati personali.

In ossequio ai criteri di delega, il decreto si compone di una parte meramente ricognitiva di norme già vigenti che prevedono obblighi di pubblicazione, per la p.a., di atti, documenti, dati e informazioni. Sotto questo profilo, l'art. 4, comma 5, del decreto riproduce integralmente il disposto dell'art. 19, comma 3-*bis*, del Codice, concernente l'accessibilità delle notizie sullo svolgimento delle prestazioni di chiunque sia addetto a una funzione pubblica e la relativa valutazione (che è stato contestualmente abrogato). Diverse sono poi le disposizioni innovative, volte a coordinare nel predetto testo unico quelle già esistenti e a stabilire principi e regole utili ad assicurare piena attuazione al principio della trasparenza.

Il decreto individua, nel Capo I, i principi generali in materia e, nei restanti capi, gli obblighi di trasparenza concernenti l'organizzazione e l'attività delle pp.aa., anche in settori particolari, nonché le misure in tema di vigilanza sull'attuazione delle disposizioni e l'impianto sanzionatorio. Per quanto riguarda l'ambito soggettivo, il decreto si applica alle amministrazioni di cui all'articolo 1, comma 2, d.lgs. n. 165/2001, in coerenza con quanto previsto dalla legge di delega (art. 1, commi 36 e 59, l. n. 190/2012). Si prevede, inoltre, che le autorità indipendenti provvedano all'attuazione di quanto previsto dalla normativa vigente in materia di trasparenza "secondo le disposizioni dei rispettivi ordinamenti". Al riguardo il Garante ha tempestivamente disciplinato con proprio regolamento gli obblighi di pubblicazione concernenti l'attività e l'organizzazione dell'Autorità (reg. 1° agosto 2013, in G.U. del 19 agosto 2013, n. 193, doc. web n. 2573442) e ha individuato i termini di pubblicazione dei dati e dei documenti (delibera 17 ottobre 2013, n. 455, doc. web n. 2753146) (cfr. par. 20.2).

Fra le disposizione recanti principi generali assumono particolare importanza sotto il profilo della protezione dei dati personali gli artt. 4, 7, 8 e 9, concernenti rispettivamente i limiti alla trasparenza, le garanzie in punto di riutilizzo dei dati e la disciplina dei termini di conservazione e dell'accesso alle informazioni. Su tali profili – come pure su altri aspetti riguardanti la protezione dei dati personali – il Garante si è espresso in occasione del parere reso, a richiesta del Governo, sullo schema di decreto, in relazione al quale si veda più approfonditamente il successivo par. 3.2.2).

3 I rapporti con il Parlamento e le altre Istituzioni

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

A. Nel 2013 l'Autorità ha fornito la consueta collaborazione al Governo con riferimento ad atti di sindacato ispettivo e ad attività di indirizzo e di controllo del Parlamento riguardanti aspetti di specifico interesse in materia di protezione dei dati personali.

In tale cornice, sono stati forniti elementi di valutazione ai fini della risposta, da parte del Governo, su quattro atti di sindacato ispettivo tutti concernenti la vicenda dei controlli statunitensi nell'ambito del programma Prism della *National Security Agency* (Nsa). Si tratta, in particolare, dei seguenti atti: a) interpellanza urgente n. 2-00104 dell'on. Quintarelli ed altri (nota 19 giugno 2013); b) interrogazione a risposta scritta n. 4-00827 dell'on. Liuzzi (nota 12 agosto 2013); c) interrogazione a risposta in commissione n. 5-00498, dell'on. Lattuca (nota 22 novembre 2013); d) interrogazione a risposta scritta n. 4-00888, dell'on. Scotto (nota 22 novembre 2013).

In tali occasioni, nel fornire propri elementi di valutazione al Governo, l'Autorità ha rappresentato vive preoccupazioni in merito ai riflessi dell'azione della Nsa, segnatamente per il carattere indiscriminato della raccolta dei dati, che coinvolge persone residenti in Europa e, sotto diverso profilo, interessa gli utenti di fornitori di servizi in rete. Il Garante ha altresì riferito che il Gruppo Art. 29 ha invitato la Commissione europea a chiedere chiarimenti sulla vicenda alle autorità statunitensi ed ha comunicato che si è tenuto a Dublino un incontro all'esito del quale è stata decisa la formazione di un gruppo transatlantico con lo scopo di raccogliere tutte le informazioni necessarie all'Unione europea per garantire la salvaguardia del diritto alla riservatezza degli interessati. L'Autorità ha inoltre fornito chiarimenti in merito al coinvolgimento dei soggetti residenti in Europa nelle attività di controllo in esame, precisando che le disposizioni previste dal Fisa (*Foreign Intelligence Surveillance Act*) consentono un trattamento rilevante di dati personali da parte delle competenti autorità federali, per motivi di sicurezza dello Stato, a prescindere dalla presenza fisica del soggetto sul territorio USA. Il Garante ha quindi rilevato che la disciplina vigente consente al soggetto che si ritenga leso nei suoi diritti da simili attività investigative di adire l'autorità giudiziaria (nel caso di specie, la *Foreign Intelligence Surveillance Court*), al fine di verificare la legittimità delle operazioni effettuate e la sussistenza dei presupposti normativi necessari allo svolgimento di tale particolare tipo di intercettazioni. In particolare, la disciplina statunitense (*minimization procedures* adottate dall'*Attorney general*, di concerto con il direttore del servizio di *intelligence*, ai sensi della *Section* 702, lett. *e*) dello US *Code*) non contempla tra i presupposti soggettivi idonei a fondare la legittimazione ad agire, anche la cittadinanza statunitense, in conformità a un indirizzo consolidato della giurisprudenza della Corte Suprema che ha da tempo ribadito come i diritti fondamentali (e le loro garanzie processuali) abbiano carattere universale e non possano quindi essere negati ai non cittadini, essendo riconosciuti alla persona in quanto tale, a prescindere dalla cittadinanza. L'Autorità ha infine osservato come resti da verificare se il diritto di azione in giudizio del cittadino non statunitense, non residente nel territorio USA, possa ritenersi effettivo in ragione delle difficoltà inevitabilmente connesse alla necessità di adire un giudice straniero in assenza peraltro degli ele-

menti probatori indispensabili ai fini di una efficace tutela giurisdizionale dei propri diritti. In tale cornice, ha altresì rammentato che l'11 novembre 2013 il Garante e il Dipartimento delle informazioni per la sicurezza (Dis) della Presidenza del Consiglio dei Ministri avevano siglato un protocollo d'intenti volto a disciplinare alcune procedure informative funzionali all'esercizio delle rispettive attribuzioni. Il protocollo prevede, in particolare, modalità di informazione idonee a consentire al Garante di conoscere alcuni elementi essenziali del trattamento dei dati personali effettuato dagli Organismi per l'informazione e la sicurezza in alcuni contesti peculiari, segnatamente quelli concernenti la sicurezza cibernetica o gli accessi alle banche dati delle pp.aa. o degli esercenti servizi di pubblica utilità (in merito cfr. par. 8.4).

B. L'Autorità si è poi interessata della problematica, di valenza più generale, concernente la diffusione dei resoconti delle attività di sindacato ispettivo e delle attività parlamentari in genere, anche in relazione al cd. diritto all'oblio dei dati personali contenuti in tali atti (cfr. *amplius* par. 16.4).

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

3.2.1. I pareri sugli atti regolamentari e amministrativi del Governo

Nel quadro dell'attività consultiva concernente norme regolamentari ed atti amministrativi suscettibili di incidere sulla protezione dei dati personali (art. 154, comma 4, del Codice; cfr. sez. IV, tab. 3), il Garante ha espresso anche nel 2013 il parere di competenza sugli schemi di numerosi provvedimenti, di seguito riportati:

1. provvedimento del Ministero della giustizia recante specifiche tecniche di cui all'art. 34 del decreto del Ministro della giustizia del 21 febbraio 2011, n. 44, in materia di tecnologie dell'informazione e della comunicazione nel processo civile e nel processo penale (parere 18 dicembre 2013, n. 584, doc. web n. 2898564);

2. regolamento riguardante determinate prescrizioni tecniche relative agli esami effettuati su tessuti e cellule umani volto a recepire la direttiva 2012/39/UE della Commissione del 26 novembre 2012 (parere 12 dicembre 2013, n. 562, doc. web n. 2851931);

3. regolamento di modifica del d.P.R. n. 378/1982 in materia di accesso del personale dei Corpi di polizia municipale e del Corpo delle capitanerie di porto a determinate informazioni registrate nel Ced interforze del Dipartimento della pubblica sicurezza (in attuazione degli artt. 16-*quater*, comma 3, d.l. n. 8/1993, convertito, con modificazioni, dalla l. n. 68/1993 e 8-*bis*, comma 3, d.l. n. 92/2008 convertito, con modificazioni, dalla l. n. 122/2008) (parere 3 ottobre 2013, n. 427, doc. web n. 2710798);

4. regolamento recante modifiche al d.P.R. 18 ottobre 2012, n. 193, in materia di "iniziativa dei cittadini", in attuazione del regolamento (UE) n. 211 del 16 febbraio 2011 (parere 19 settembre 2013, n. 404, doc. web n. 2690852);

5. decreto dirigenziale del Ministero della giustizia recante regole procedurali di carattere tecnico-operativo per la trasmissione telematica da parte dei comuni al sistema informativo del Casellario giudiziale delle informazioni concernenti le persone decedute (art. 20, comma 3, d.P.R. 14 novembre 2002, n. 313) (parere 19 settembre 2013, n. 405, doc. web n. 2849463);

6. decreto del Ministro dell'interno concernente l'organizzazione della Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza, e l'istituzione dell'ufficio per la sicurezza dei dati (parere 1° agosto 2013, n. 378, doc. web n. 2635009);

7. regolamento del Ministro dell'interno recante disposizioni in materia di carta di identità elettronica unificata alla tessera sanitaria, adottato ai sensi dell'art. 10, comma 3, d.l. 13 maggio 2011, n. 70, convertito dalla l. 12 luglio 2011, n. 106 e successive modificazioni (pareri 31 gennaio 2013, n. 39, e 27 giugno, n. 312, doc. web nn. 2275741 e 2576276);

8. regolamento del Ministro della giustizia recante disposizioni in materia di iscrizione sospensione e cancellazione dall'Albo degli amministratori giudiziari di cui al d.lgs. 4 febbraio 2010, n. 14 nonché in materia di esercizio del potere di vigilanza da parte del Ministero della giustizia (parere 27 giugno 2013, n. 314, doc. web n. 2576306);

9. linee guida dell'Agenzia per l'Italia Digitale in materia di *Disaster Recovery* delle pp.aa., emanato ai sensi dell'art. 50-*bis*, comma 3, lett. *b*), d.lgs. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale - Cad) (parere 4 luglio 2013, n. 333, doc. web n. 2563133);

10. decreto del Presidente del Consiglio dei Ministri volto all'istituzione dell'Anagrafe nazionale della popolazione residente, adottato ai sensi dell'art. 62, comma 6, del Cad introdotto dall'art. 2, comma 1, d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 121 (parere 24 aprile 2013, n. 216, doc. web n. 2448700);

11. decreto del Presidente del Consiglio dei Ministri recante regole tecniche in materia di formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pp.aa. ai sensi degli artt. 20, 22, 23-*bis*, 23-*ter*, 40, comma 1, 41 e 71, comma 1, del Cad (parere 24 aprile 2013, n. 213, doc. web n. 2460830);

12. decreto del Presidente del Consiglio dei Ministri recante regole tecniche in materia di sistema di conservazione ai sensi degli artt. 20, commi 3 e 5-*bis*, 23-*ter*, comma 4, 43, commi 1 e 3, 44, 44-*bis* e 71, comma 1, del Cad (parere 24 aprile 2013, n. 214, doc. web n. 2470970);

13. decreto del Presidente del Consiglio dei Ministri recante regole tecniche per il protocollo informatico ai sensi degli artt. 40-*bis*, 41, 47, 57-*bis* e 71, comma 1, del Cad (parere 24 aprile 2013, n. 215, doc. web n. 2471217);

14. decreto dirigenziale del Ministero della giustizia recante regole procedurali di carattere tecnico operativo per l'attuazione del sistema di interconnessione tra il Sistema informativo del Casellario giudiziale (SiC) e il Sistema integrato dell'esecuzione e della sorveglianza (Sies) (parere 18 aprile 2013, n. 198, doc. web n. 2446914);

15. decreto del Ministro dell'istruzione, dell'università e della ricerca riguardante le modalità e i contenuti delle prove di ammissione ai corsi di laurea e di laurea magistrale ad accesso programmato per l'anno accademico 2013-2014 (parere 11 aprile 2013, n. 176, doc. web n. 2422263);

16. regolamento del Ministro dell'economia e delle finanze volto a disciplinare il sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità (parere 21 marzo 2013, n. 135, doc. web n. 2462626), in merito al quale, attesa la complessità del sistema e i suoi possibili effetti sulla protezione dei dati personali, una sintetica disamina del parere reso dal Garante, i cui contenuti hanno trovato eco nel parere del Consiglio di Stato del 31 ottobre 2013, n. 4471, è svolta al termine del presente paragrafo (p. 25 ss.);

17. decreto del Ministro della salute concernente le modalità tecniche per la realizzazione della infrastruttura di rete per il supporto all'organizzazione delle attività libero professionale intramuraria (art. 1, comma 4, quarto periodo, lett. a-*bis*, l. 3 agosto 2007, n. 120) (parere 14 febbraio 2013, n. 63, doc. web n. 2279266);

18. decreto del Ministro dell'istruzione, dell'università e della ricerca recante le modalità di prova di ammissione al corso di laurea magistrale in medicina e chirurgia in inglese (parere 14 febbraio 2013, n. 62, doc. web n. 2304831);

19. decreto del Ministro dell'istruzione, dell'università e della ricerca riguardante le modalità di effettuazione delle preiscrizioni da parte degli studenti iscritti all'ultimo anno delle scuole secondarie superiori, interessati all'accesso ai corsi di istruzione superiore (parere 31 gennaio 2013, n. 40, doc. web n. 2300643);

20. regolamento recante integrazione dell'art. 49, d.P.R. 31 agosto 1999, n. 394 (di attuazione del testo unico delle disposizioni in materia di immigrazione e condizione dello straniero), volto a disciplinare il riconoscimento in Italia dei titoli abilitanti all'esercizio della professione medica conseguiti in un Paese extra-UE, ai fini dell'esercizio temporaneo dell'attività (parere 17 gennaio 2013, n. 12, doc. web n. 2298861);

21. decreto del Ministro del lavoro e delle politiche sociali concernente la costituzione, presso l'Istituto nazionale della previdenza sociale (Inps), della banca dati delle prestazioni sociali agevolate, adottato ai sensi dell'art. 5, comma 1, d.l. 6 dicembre 2011, n. 201, convertito dalla l. 22 dicembre 2011, n. 214 (parere 17 gennaio 2013, n. 14, doc. web n. 2300596).

Mancata consultazione del Garante

A fronte dei pareri sopra menzionati, continuano tuttavia a registrarsi casi di mancata consultazione dell'Autorità in relazione a provvedimenti che, ancorché (talvolta) non prevedano specifiche disposizioni in materia di protezione dei dati personali, in ogni caso, incidono su tale materia. Tra questi provvedimenti si richiamano, in particolare, i seguenti:

1) il decreto del Ministero delle infrastrutture e dei trasporti 15 novembre 2013 recante disposizioni procedurali attuative degli artt. 1, 2 e 3 del d.m. 9 agosto 2013 in materia di nuove procedure di comunicazione del rinnovo di validità della patente (in G.U. 10 dicembre 2013, n. 289);

2) il decreto del Ministro dello sviluppo economico 9 agosto 2013, n. 110, recante il regolamento sulle norme per la progressiva dematerializzazione dei contrassegni di assicurazione per la responsabilità civile verso i terzi per danni derivanti dalla circolazione dei veicoli a motore su strada, attraverso la sostituzione degli stessi con sistemi elettronici o telematici, di cui all'art. 31, d.l. 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla l. 24 marzo 2012, n. 27 (in G.U. 3 ottobre 2013, n. 232);

3) il decreto del Ministro delle infrastrutture e dei trasporti 9 agosto 2013 recante disciplina dei contenuti e delle procedure della comunicazione del rinnovo di validità della patente (in G.U. 2 ottobre 2013, n. 231);

4) il decreto del Ministro della salute 6 agosto 2013 recante modifica del d.m. 9 luglio 2012, recante contenuti e modalità di trasmissione delle informazioni relative ai dati aggregati sanitari e di rischio dei lavoratori, ai sensi dell'art. 40, d.lgs. 9 aprile 2008, n. 81, in materia di tutela della salute e della sicurezza nei luoghi di lavoro (in G.U. 10 settembre 2013, n. 212);

5) il decreto del Ministro delle infrastrutture e dei trasporti 1° febbraio 2013, recante la diffusione dei sistemi di trasporto intelligenti (ITS) in Italia (in G.U. 26 marzo 2013, n. 72).

Prevenzione delle frodi, credito al consumo e furto d'identità

Come anticipato, uno schema di regolamento del Ministro dell'economia e delle finanze (di seguito Mef) volto a disciplinare il sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità, ha formato oggetto di valutazione da parte del Garante con il parere 21 marzo 2013, n. 135 (doc. web n. 2462626). Rispetto a tale sistema di prevenzione, istituito dal d.lgs. 11 aprile 2011, n. 64 (che ha integrato al riguardo il d.lgs. n. 141/2010) – in termini non dissimili da quanto previsto da un testo normativo precedentemente discusso in Parlamento e in relazione al quale il

Garante aveva espresso alcune perplessità di fondo nel corso di due audizioni tenute presso le competenti commissioni parlamentari (nel 2008 e nel 2009) – il progetto iniziale il sistema di prevenzione era disegnato come mero "snodo tecnico", apprestato presso il Mef, attraverso il quale il gestore doveva provvedere a riscontrare le richieste di verifica provenienti dai soggetti aderenti al sistema (banche, essenzialmente) su dati e informazioni registrati in altre, distinte banche dati. Ciò al fine di controllare la "veridicità" dei dati personali identificativi dei soggetti che ricorrono al credito al consumo, al fine di scoraggiare fenomeni di sostituzione di persona (mediante falsificazione di documenti o altre pratiche in frode alla legge) largamente diffusi, purtroppo, per poter avere accesso al credito. Senonché, l'originario impianto del progetto normativo e la configurazione del sistema sono stati snaturati già nel corso dei lavori in Parlamento, affiancandosi allo "snodo tecnico" un vero e proprio archivio presso il Mef.

Infatti, in base alla disposizione normativa vigente (art. 30-*quater*, d.lgs. n. 141/2010) il sistema di prevenzione è basato su un "archivio centrale informatizzato", composto, oltre che da una "interconnesione di rete" (lo snodo tecnico di cui sopra), anche da un "modulo informatico di allerta" nel quale sono memorizzate, fra l'altro, le informazioni trasmesse dai soggetti aderenti al sistema relative alle frodi subite e ai casi che configurano un rischio di frodi. Il Garante ha perciò ribadito, nella premessa del parere, le proprie perplessità sull'istituzione di una banca dati di così grandi dimensioni, contenente numerose e delicate informazioni sui cittadini che ricorrono al credito o ad altri servizi, i quali rischiano così di essere oggetto di pericolose stigmatizzazioni sulla base di una valutazione rimessa, fra l'altro, anche agli stessi operatori del settore, piuttosto che alle pubbliche autorità competenti in materia di prevenzione e repressione di comportamenti fraudolenti.

L'Autorità, perciò, pur prendendo atto che le finalità sottese all'esigenza di prevenire l'uso indebito di informazioni e documenti a fini fraudolenti sono lecite e svolte a garanzia delle persone interessate (possibili frodati), ha tuttavia rilevato la necessità di un equo bilanciamento di tali esigenze con i diritti delle persone, in quanto, in ogni caso, il trattamento dei dati personali che si rende necessario a tali fini può presentare "rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità" degli interessati, che richiedono un'attenta valutazione (art. 17 del Codice).

Il Garante, quindi, a prescindere dalle cautele ipotizzate nello schema di regolamento si è riservato la facoltà di prescrivere autonomamente altre misure ed accorgimenti che si rivelassero necessari a garanzia degli interessati, anche sulla base della prima esperienza applicativa (art. 17 del Codice).

Nel parere ha poi confermato un'altra criticità, già oggetto di precedente segnalazione al Parlamento: l'allargamento della "partecipazione" al sistema ad una vasta platea di soggetti (definiti aderenti, diretti o indiretti), per giunta per finalità non ben identificate e in alcuni casi diverse da quelle di valutazione del merito creditizio. Si pensi, ad esempio, ai fornitori di servizi di comunicazione elettronica o di servizi interattivi, come pure ai "gestori di sistemi di informazioni creditizie", oppure ancora, alle imprese di assicurazione, "aggiunte" dal d.lgs. n. 164/2012.

Quanto al contenuto del regolamento, l'Autorità ha subordinato il parere favorevole ad una serie di condizioni volte a rendere il testo conforme ai principi e alle regole in materia di protezione dei dati personali. Tale condizioni hanno riguardato in particolare l'esigenza:

a) di esplicitare nello schema di provvedimento, o comunque di tener conto nella fase di attuazione, delle finalità del trattamento e dell'ambito applicativo del regolamento che riguarda, inequivocabilmente, le frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità.

La disciplina in esame non riguarda i casi di alterazione di documenti propri o altri comportamenti fraudolenti che non comportino la sostituzione di persona (anche parziale). Ad esempio, quindi, non sarebbe assoggettabile alla disciplina del decreto la contraffazione del solo elemento reddituale presente nella propria dichiarazione dei redditi o busta paga;

b) di prevedere espressamente che gli aderenti diretti (banche, intermediari finanziari e gli altri soggetti previsti dalla legge) partecipino al sistema di prevenzione esclusivamente in relazione ai dati, pertinenti e non eccedenti, necessari al perseguimento delle specifiche finalità inerenti al settore commerciale di appartenenza;
c) di precisare il ruolo riservato agli aderenti indiretti (i gestori di sistemi di informazioni creditizie e le imprese che offrono agli aderenti diretti servizi assimilabili alla prevenzione, sul piano amministrativo, delle frodi, in base ad apposita convenzione con il Mef) nel funzionamento del sistema e i connessi limiti al trattamento dei dati personali;
d) di assicurare che i dati sottoposti a verifica siano riscontrati, tramite l'apposita interfaccia informatica, presso le banche dati delle amministrazioni "titolari" dei dati stessi (amministrazioni "certificanti"), al fine di garantire la correttezza del trattamento dei dati e la loro esattezza, nonché per evitare pericolosi disallineamenti informativi (si consideri la recente istituzione, presso il Ministero dell'interno, dell'Anagrafe nazionale della popolazione residente);
e) di integrare le informazioni relative alle frodi subite e al rischio di frodi che gli aderenti diretti devono immettere nell'archivio con il "motivo della segnalazione" cui è connessa la frode o il rischio di frode, al fine di scongiurare accessi abusivi al sistema;
f) di prevedere che al momento della richiesta di credito o di altro servizio debba essere fornita, a cura dell'aderente diretto, un'informativa ai sensi dell'art. 13 del Codice, specifica in ordine al trattamento dei dati effettuato per finalità antifrode;
g) di integrare l'allegato tecnico con la previsione di misure di sicurezza, tecniche e organizzative, idonee ad assicurare un livello elevato di sicurezza nella protezione dei dati personali.

3.2.2. Gli altri pareri

Il Garante ha reso inoltre il proprio parere, su espressa richiesta del Governo, anche su altri atti normativi aventi rango primario e in particolare sui seguenti:

A. Con il provvedimento del 7 febbraio 2013, n. 49 (doc web. n. 2243168) il Garante ha reso il proprio parere sullo schema di decreto legislativo concernente il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pp.aa. (poi adottato dal Governo: d.lgs. 14 marzo 2013, n. 33: v. par. 2.1.2). L'esame del Garante ha riguardato principalmente le disposizioni dello schema concernenti il regime di pubblicità riservato alle informazioni personali, al fine di valutarne la compatibilità con la disciplina, anche comunitaria, in materia di protezione dei dati personali.

Il tema della trasparenza (o comunque della diffusione di informazioni) riveste infatti grande importanza per le autorità di protezione dei dati personali per quanto riguarda il contemperamento di tale principio con la disciplina in materia di protezione dei dati personali, contenuta anzitutto nella direttiva 95/46/CE, come interpretata ed applicata dalla giurisprudenza della Corte di giustizia

dell'Unione europea (cfr., in particolare, sentenza 9 novembre 2010, cause riunite C-92/09 e C-93/09).

L'espressione del parere è stata un'occasione preziosa per il Garante per contribuire in maniera sistematica al bilanciamento di valori costituzionali così importanti, come la trasparenza, la riservatezza degli individui e la protezione dei loro dati personali, tenuto conto, peraltro, dell'ambito di applicazione del decreto che mira a disciplinare in maniera organica i casi di pubblicazione di dati sui siti istituzionali, cioè mediante diffusione sul web, che è, per definizione, la forma più ampia e più invasiva di diffusione di dati.

I rischi connessi al trattamento dei dati personali sulla rete emergono ancora di più ove si consideri la delicatezza di talune informazioni e la loro facile reperibilità una volta pubblicate, grazie anche ai motori di ricerca; si consideri anche il rischio di "cristallizzazione" delle informazioni sul web, a fronte di oggettive difficoltà pratiche (oltre che giuridiche, a volte) nell'ottenere la loro cancellazione una volta decorso il termine di pubblicazione e, soprattutto, laddove un termine non sia fissato o comunque i dati non siano cancellati dopo il raggiungimento dello scopo perseguito, in violazione del cd. diritto all'oblio.

In questo quadro, l'Autorità ha rilevato l'esigenza di allineare il testo dell'articolato alla disciplina comunitaria e nazionale in materia di protezione dei dati personali, fornendo indicazioni su diversi aspetti rilevanti.

L'Autorità ha segnalato, in particolare, la necessità:

a) che fossero rispettati i principi di necessità e di pertinenza nel trattamento dei dati personali (artt. 3 e 11 del Codice), prevedendo espressamente l'obbligo per la p.a., al momento della pubblicazione del documento o dell'atto, di rendere comunque non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione, nonché di ricorrere sempre a forme di anonimizzazione dei dati personali eventualmente presenti nel documento in caso di pubblicazione "facoltativa" (art. 4, commi 3 e 4);
b) che la rintracciabilità dei dati fosse ammessa solo con motori di ricerca interni ai siti istituzionali ove i documenti e le informazioni sono pubblicati, e non mediante motori di ricerca web e indicizzazione delle informazioni; ciò, sul presupposto che un obbligo indifferenziato e ampio, come quello previsto dallo schema, fosse contrario al principio di proporzionalità nel trattamento dei dati, e incidesse negativamente sull'esigenza di avere dati esatti, aggiornati e, soprattutto, contestualizzati;
c) di prevedere espressamente il divieto assoluto di diffusione non solo di dati idonei a rivelare lo stato di salute, ma anche di quelli sulla vita sessuale degli individui;
d) del rispetto delle garanzie previste dal Codice in punto di riutilizzo dei dati personali in altre operazioni di trattamento, che è consentito solo in termini compatibili con gli scopi per i quali sono stati originariamente raccolti e registrati (art. 11, comma 1, lett. *b*), del Codice);
e) di prevedere termini differenziati di pubblicazione delle informazioni in ragione delle categorie di dati e delle specifiche finalità della pubblicazione (in luogo di quello, unico, di 5 anni proposto nello schema) e di chiarire, anche a beneficio dei soggetti pubblici interessati all'applicazione del decreto, gli adempimenti da mettere in opera alla scadenza del termine. La generica previsione dell'art. 9, comma 2, secondo cui alla scadenza del termine i dati e documenti devono essere conservati in altre sezioni del sito e resi comunque disponibili (peraltro rimasta immutata nel testo appro-

vato dal Governo) avrebbe finito col vanificare, di fatto, la pubblicazione temporanea delle informazioni stabilita al precedente art. 8 con l'apposizione di un termine, in violazione del "diritto all'oblio" (cfr. Corte di Giustizia 9 novembre 2010, cause riunite C-92/09 e C-93/09); l'Autorità ha perciò richiesto di prevedere quanto meno un'accessibilità selettiva e mirata dei documenti e dei dati dopo la scadenza del termine di pubblicazione, sancendo espressamente la cancellazione dei dati personali;

f) di introdurre selettivamente, in relazione alla prevista pubblicazione di dati concernenti i titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico (art. 14), una graduazione degli obblighi di pubblicazione, sia sotto il profilo della platea dei soggetti coinvolti, che del contenuto degli atti da pubblicare. Occorre infatti considerare che il decreto modifica, con interventi mirati, la l. n. 441/1982 estendendo il novero dei soggetti titolari di incarichi pubblici cui è rimesso l'obbligo di trasparenza, sino a ricomprendervi anche: i vice ministri, i componenti della giunta regionale e provinciale, i consiglieri dei comuni con popolazione superiore a 15.000 abitanti (rispetto ai 50.000 attuali), fermi restando in ogni caso i capoluoghi di provincia. Sotto questo profilo l'Autorità ha suggerito differenziazioni fra organi locali e nazionali oppure, per quanto riguarda le autonomie, fra le cariche elettive e i livelli di governo (consiglieri e assessori). Quanto ai soggetti diversi dal titolare dell'incarico pubblico, il riferimento normativo è al coniuge non separato e ai parenti entro il secondo grado, ove vi consentano. Da questo punto di vista quindi l'ambito di applicazione della trasparenza è esteso ai figli, anche non conviventi, ai fratelli e ai genitori del titolare dell'incarico pubblico. L'Autorità ha perciò osservato nel parere che la disciplina complessiva che il Governo intendeva introdurre appariva sproporzionata rispetto alle finalità di trasparenza che lo stesso provvedimento normativo si prefiggeva. Si consideri, infatti, l'invasività della pubblicazione mediante diffusione sul web, rispetto a una massa enorme di informazioni che in alcuni casi possono rivelare aspetti, anche intimi, della vita privata delle persone, soprattutto se ci si riferisce al coniuge, ai figli e ai parenti, che sono estranei all'incarico pubblico (si pensi ai possibili risvolti sociali di una lettura mirata, se non tendenziosa, del reddito e della consistenza patrimoniale dei soggetti, specie in ambiti territoriali ristretti, e ai connessi rischi di discriminazione sociale). Per quanto riguarda tali soggetti ("terzi" rispetto all'incarico pubblico), il Garante ha richiesto di circoscrivere il contenuto delle dichiarazioni sulla situazione patrimoniale assicurando altresì l'espressione di un consenso alla pubblicazione dei dati effettivamente libero e reso in assenza di condizionamenti. Infatti, poiché la norma prevedeva (e purtroppo prevede ancora) di dare "evidenza al mancato consenso" del coniuge e dei parenti alla pubblicazione delle dichiarazioni, l'Autorità ha rilevato che ciò avrebbe esposto tali soggetti a pericolose stigmatizzazioni in caso di mancata espressione del consenso e ha perciò chiesto la soppressione di tale disposizione, peraltro non prevista dall'art. 1, comma 35, lett. *c*), della legge di delega n. 190/2012;

g) di circoscrivere la pubblicazione obbligatoria dei dati relativi a dipendenti pubblici (artt. 15, 16 e 18) a un novero più ristretto di informazioni personali, strettamente pertinenti, e individuando modalità di diffusione dei dati che, pur consentendo un controllo diffuso sull'attività della p.a. per assicurarne il buon andamento, risultino meno invasive della sfera personale;

h) di escludere espressamente dall'obbligo di pubblicazione i dati identificativi dei destinatari di provvedimenti riguardanti persone fisiche dai quali sia possibile evincere informazioni relative allo stato di salute degli interessati, ovvero lo stato economico-sociale disagiato degli stessi (cfr. art. 26, comma 4). Da questo punto di vista il Garante, anche alla luce del contesto normativo (contrasto della corruzione, in particolare per quanto riguarda le concessioni di appalti o l'affidamento di lavori e forniture) ha sottolineato l'esigenza di non applicare lo specifico obbligo di trasparenza a ogni forma di sussidio, contributo o vantaggio economico previsto per il cittadino, come ad esempio quelli nel campo della solidarietà sociale (si pensi alla *Social card*) i cui procedimenti sono spesso idonei a rivelare lo stato di salute dei beneficiari del contributo o comunque situazioni di particolare bisogno o disagio sociale (in tal senso si pensi al riconoscimento di agevolazioni economiche, nella fruizione di prestazioni sociali, collegate alla situazione reddituale come l'esenzione dal contributo per la refezione scolastica o l'esenzione dal pagamento del cd. *ticket* sanitario). Fermo restando che deve essere comunque rispettato il divieto di pubblicare dati idonei a rivelare lo stato di salute (art. 22, comma 8, del Codice), l'eventuale diffusione sul web di altre informazioni sensibili o comunque idonee ad esporre l'interessato a discriminazioni, presenta rischi specifici per la dignità degli interessati, che spesso versano in condizioni di disagio economico-sociale. Si pensi a dati particolarmente delicati, che non appaiono pertinenti rispetto alle finalità perseguite, quali l'indirizzo di abitazione, il codice fiscale, le coordinate bancarie dove sono accreditati i contributi, la ripartizione degli assegnatari secondo le fasce dell'Indicatore della situazione economica equivalente-Isee ovvero informazioni che descrivano le condizioni di indigenza in cui versa l'interessato.

Non tutte le indicazioni del Garante sono state tenute in considerazione dal Governo nell'elaborazione del testo poi approvato, in particolare per quanto riguarda l'utilizzo dei motori di ricerca, la durata della pubblicazione e l'accesso alle informazioni pubblicate nei siti. Ma ciò che più rileva – ad avviso della Autorità – è che è mancata la richiesta riflessione generale sull'impianto della disciplina in esame e sull'opportunità di una graduazione selettiva degli obblighi di pubblicazione sotto il profilo della platea dei soggetti coinvolti (titolari di incarichi politici, coniuge, parenti, dipendenti pubblici ed equiparati) e del contenuto degli atti da pubblicare (artt. 14, 15 e 18).

B. Il Garante ha reso altresì parere su uno schema di disegno di legge di ratifica ed esecuzione della Convenzione internazionale per la protezione delle persone scomparse (cd. sparizioni forzate), adottata dall'Assemblea generale delle Nazioni Unite il 20 dicembre 2006 (parere 18 dicembre 2013, n. 585, doc. web n. 2896494).

3.3. *L'esame delle leggi regionali*

Nel 2013 è proseguita l'attività di esame e valutazione 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 per i profili connessi alla protezione dei dati personali.

Sono state così esaminate 16 leggi regionali e forniti elementi alla Presidenza del Consiglio dei Ministri in merito alla compatibilità con le disposizioni in materia di

protezione dei dati personali e con il dettato costituzionale (art. 117, comma 2, lett. *l*), Cost.) per la legge Regione Abruzzo 1° ottobre 2013, n. 31, recante la legge organica sul procedimento amministrativo. In particolare, l'art. 31, comma 1, lett. *c*), ptevede che il diritto di accesso sia riconosciuto a tutti senza obbligo di motivazione. L'Autorità ha segnalato come detta disposizione sembra porsi in contrasto con la disciplina sul diritto di accesso ai documenti amministrativi recata dalla l. n. 241/1990 (e, conseguentemente, con il Codice), che prevede la motivazione della richiesta di accesso (art. 25, comma 2), anche allo scopo di tutelare i controinteressati, titolari del diritto alla riservatezza e alla protezione dei dati personali (art. 22, comma 1, lett. *c*). La motivazione evidenzia, infatti, la sussistenza della situazione giuridicamente tutelata e connessa all'oggetto della richiesta di accesso che rappresenta, al contempo, il termine di riferimento con cui comparare i diritti del controinteressato, al fine di valutare la prevalenza o meno del diritto di accesso rispetto alla tutela della riservatezza e del diritto alla protezione dei dati personali di quest'ultimo. L'Autorità ha posto in luce come il legislatore statale, nel dettare la disciplina della prorezione dei dati personali di cui agli artt. 59 e 60 del Codice, abbia previsto la motivazione della richiesta di accesso segnatamente allo scopo di far emergere, ove sussistente, quella situazione giuridicamente tutelata, la cui cura o difesa necessiti dell'accesso a documenti contenenti dati personali comuni (art. 24, comma 7, l. n. 241/1990); o per la cui tutela sia strettamente indispensabile l'accesso a documenti contenenti dati sensibili e giudiziari (art. 24, comma 7, l. n. 241/1990); ovvero per la cui salvaguardia occorra accedere a documenti recanti dati cd. super sensibili (inerenti allo stato di salute o alla vita sessuale), ove detta situazione giuridicamente rilevante per l'ordinamento sia "di rango almeno pari ai diritti dell'interessato", o consista in "un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile" (artt. 24, comma 7, l. n. 241/1990 e 60 del Codice).

PAGINA BIANCA

L'attività svolta dal Garante

PAGINA BIANCA

II - L'attività svolta dal Garante

4 Il Garante e le pubbliche amministrazioni

4.1. *I regolamenti sui trattamenti di dati sensibili e giudiziari*

Nel 2013 il Garante ha espresso parere favorevole sullo schema tipo aggiornato di regolamento per il trattamento di dati sensibili e giudiziari presso i consigli e le assemblee legislative delle Regioni e delle Province autonome (provv. 25 luglio 2013, n. 370, doc. web n. 2576905). La revisione dello schema tipo è stato frutto di un complesso e proficuo lavoro di collaborazione dell'Autorità con la Conferenza dei presidenti delle assemblee legislative delle Regioni e delle Province autonome. Il nuovo testo, predisposto dalla Conferenza, tiene conto della necessità di adeguare i regolamenti regionali sul trattamento di dati sensibili e giudiziari al mutato quadro normativo in vari settori di attività di competenza dei consigli e delle assemblee legislative.

A tale proposito, come è noto, il Codice prevede che, per poter trattare dati sensibili e giudiziari indispensabili allo svolgimento delle attività istituzionali, le Regioni e le Province autonome – non diversamente dagli altri soggetti pubblici – debbano dotarsi di specifici regolamenti volti a individuare quali informazioni vengono utilizzate, per quali finalità e mediante quali operazioni di trattamento (artt. 20 e 21 del Codice).

Al riguardo, sin dal 2005 il Garante ha intrapreso un'attività di collaborazione con la Conferenza dei presidenti delle assemblee legislative delle Regioni e delle Province autonome che ha condotto, in un primo tempo, all'elaborazione di un primo schema tipo di regolamento, sul quale l'Autorità ha espresso un parere condizionato al rispetto di alcune indicazioni (provv. 29 dicembre 2005, doc. web n. 1210939), successivamente modificato ed integrato (in merito cfr. il parere condizionato adottato con provv. 12 giugno 2008, doc. web n. 1537639); nel corso del 2013 è stato poi approntato uno schema tipo aggiornato di regolamento che ha tenuto conto degli approfondimenti e delle indicazioni suggeriti dall'Ufficio in via collaborativa, volti a perfezionare il testo e a renderlo pienamente conforme alla disciplina in materia di protezione dei dati personali: le osservazioni formulate hanno riguardato, tra l'altro, il rispetto dei principi di pertinenza e non eccedenza nel trattamento dei dati sensibili di titolari di incarichi politici e di vertice, nonché di incarichi dirigenziali, di collaborazione e di consulenza in attuazione degli obblighi di pubblicazione previsti dalla disciplina in materia di trasparenza e di contrasto della corruzione; le cautele da adottare nel trattamento delle informazioni sulla vita sessuale delle persone soggette a misure restrittive della libertà personale da parte dai Garanti regionali per i diritti dei detenuti; i limiti da rispettare nell'utilizzo di dati sensibili e giudiziari di terzi nell'ambito delle attività di sindacato ispettivo, di indirizzo politico e di documentazione dell'attività istituzionale dei consigli e delle assemblee legislative.

Ciononostante, nell'esprimere il parere, l'Autorità ha chiesto l'integrazione dello schema con la previsione di specifiche garanzie in tema di accesso dei consiglieri regio-

nali a documenti amministrativi; in particolare, il Garante ha richiesto di specificare che le istanze di accesso ai documenti da parte dei consiglieri possano essere accolte solo se riconducibili alle "esclusive" finalità di rilevante interesse pubblico "direttamente connesse all'espletamento di un mandato elettivo" (art. 65, comma 4, del Codice) e che possano essere soddisfatte soltanto con modalità tali da assicurare che l'accesso del consigliere comporti il minor pregiudizio possibile alla vita privata delle persone cui si riferiscono i dati contenuti nei documenti oggetto dell'istanza di accesso. Ciò anche al fine di garantire che il diritto di accesso in questione sia esercitato con riguardo ai dati effettivamente utili per l'esercizio del mandato, fermo restando che i dati personali eventualmente acquisiti dal consigliere possono essere utilizzati per le sole finalità realmente pertinenti al mandato (cfr. provv. 25 luglio 2013, n. 369, doc. web n. 2536172, illustrato *infra* par. 4.3).

4.2. *Le grandi banche dati pubbliche*

Linee guida AgID (art. 58, comma 2, del Cad)

Il Garante ha espresso parere favorevole sulle linee guida redatte dall'Agenzia per l'Italia Digitale (AgID) ai sensi dell'art. 58, comma 2, d.lgs. 7 marzo 2005, n. 82 (Cad), il quale prevede che le amministrazioni titolari di banche dati accessibili per via telematica predispongano apposite convenzioni, aperte all'adesione di tutte le amministrazioni interessate, volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti, senza oneri a loro carico (provv. 4 luglio 2013, n. 332, doc. web n. 2574977).

Nell'aprile 2011, DigitPA, ora AgID, aveva pubblicato una prima versione delle predette linee guida in relazione alle quali, in collaborazione con l'Ufficio, erano state apportate modifiche e integrazioni volte, in particolare, a migliorare gli aspetti relativi alle convenzioni aventi per oggetto l'accesso a dati personali e a rendere conformi alla disciplina in materia di protezione dei dati personali i trattamenti ivi previsti.

Il testo, modificato nel 2013, oltre a prevedere il necessario rispetto delle misure minime di sicurezza previste dal Codice (art. 33), reca anche le misure necessarie prescritte dal Garante ai destinatari delle linee guida ("erogatore" e "fruitore" dei dati) al fine di ridurre al minimo i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento (art. 31 del Codice), salvo che le convenzioni medesime o le modalità di accesso alle banche dati siano già state oggetto di esame da parte del Garante nell'ambito di specifici provvedimenti.

In caso di convenzioni già stipulate ai sensi del predetto art. 58, comma 2, del Cad, anteriormente all'adozione delle nuove linee guida, le misure necessarie individuate nel provvedimento dovranno essere adottate in occasione del rinnovo delle stesse e, comunque, entro e non oltre il 30 giugno 2014.

Il Garante ha ritenuto altresì necessario che l'AgID segnali all'Autorità le difformità relative agli aspetti di sicurezza e protezione dei dati personali rilevate nell'ambito dei controlli effettuati dall'Agenzia stessa sulle convenzioni-quadro e metta a disposizione del Garante, per via telematica, un documento aggiornato contenente i dati relativi alle convenzioni, al fine di agevolare le procedure di controllo dell'Autorità, anche in coordinamento con la medesima Agenzia.

Le misure necessarie prescritte dal Garante hanno riguardato, in particolare, le modalità d'accesso e gli aspetti di protezione dei dati personali, individuando anche accorgimenti volti ad assicurare la correttezza del trattamento e a ridurre rischi nell'utilizzo dei dati personali, con specifica attenzione ai presupposti per l'accesso alle

banche dati verificandone periodicamente la base normativa, le finalità istituzionali perseguite dal fruitore, la natura e la qualità dei dati richiesti. Deve essere inoltre prescelta la modalità telematica di accesso alle banche dati più idonea rispetto alle caratteristiche anche infrastrutturali e organizzative del fruitore, al volume e alla frequenza dei trasferimenti, al numero di soggetti abilitati all'accesso, offrendo – nel rispetto dei principi di pertinenza e non eccedenza in relazione a ciascuna delle finalità perseguite dal fruitore – un livello minimo di accesso ai dati, anche limitando i risultati delle interrogazioni a valori di tipo booleano (ad es., *web service* che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un dato oggetto di autocertificazione).

Per la cooperazione applicativa, viene specificato che i *web service* devono essere integrati soltanto in applicativi che gestiscono procedure amministrative volte al raggiungimento delle finalità istituzionali per le quali è consentita la comunicazione delle informazioni contenute nella banca dati. In ogni caso, il fruitore deve garantire che i servizi resi disponibili dall'erogatore vengano esclusivamente integrati con il proprio sistema informativo e che non siano resi disponibili a terzi per via informatica.

Oltre a garantire il rispetto delle misure minime di sicurezza previste dagli artt. 33 e ss. del Codice, e dal relativo Allegato B, al fine di adempiere agli obblighi di sicurezza di cui all'art. 31 del Codice, per quanto riguarda la fruibilità dei dati oggetto della convenzione (sia in caso di accessi via web che di cooperazione applicativa), l'erogatore e il fruitore devono assicurare, in particolare, che gli accessi alle banche dati avvengano soltanto tramite l'uso di postazioni di lavoro connesse alla rete *Ip* dell'ente autorizzato e/o dotate di certificazione digitale in modo che sia identificata univocamente la postazione di lavoro nei confronti dell'erogatore, anche attraverso procedure di accreditamento che consentano di definire reti di accesso sicure (circuiti privati virtuali).

Inoltre, i sistemi *software*, i programmi utilizzati e la protezione antivirus devono essere costantemente aggiornati sia sui *server* che sulle postazioni di lavoro e, in caso di accessi via web, deve essere di regola esclusa la possibilità di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse.

Tutte le operazioni di trattamento di dati personali effettuate dagli utenti autorizzati, ivi comprese le utenze di tipo applicativo e sistemistico, devono poi essere adeguatamente tracciate e il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata, il codice identificativo dell'utenza che ha posto in essere l'operazione; codice che, anche nel caso in cui l'accesso avvenga attraverso sistemi di cooperazione applicativa, deve essere comunque univocamente riferito al singolo utente incaricato del trattamento che ha dato origine alla transazione.

L'erogatore e il fruitore devono predisporre idonee procedure di *audit* sugli accessi alle banche dati basate sul monitoraggio statistico delle transazioni e su meccanismi di *alert* che individuino comportamenti anomali o a rischio, i cui esiti devono essere documentati secondo le modalità definite nelle convenzioni.

A tal fine, nelle applicazioni volte all'uso interattivo da parte di incaricati deve essere inserito un campo per l'indicazione obbligatoria del numero di riferimento della pratica (ad es., numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.

È comunque compito dell'erogatore valutare l'introduzione di eventuali ulteriori misure e accorgimenti al fine di salvaguardare la sicurezza dei propri sistemi informativi, anche in considerazione delle caratteristiche delle banche dati accessibili attraverso la convenzione (ad es., delicatezza e rilevanza delle informazioni accedute, rilevanti dimensioni della banca dati o del numero di utenti o del volume di trasferimenti).

Banca nazionale dei contratti pubblici

Il Garante ha espresso parere favorevole sulle modifiche alla deliberazione n. 111/2012 dell'Autorità per la Vigilanza sui Contratti Pubblici (AVCP) concernente il trattamento dei dati nell'ambito della Banca nazionale dei contratti pubblici (parere 1° agosto 2013, n. 377, doc. web n. 2576925).

Le modifiche, finalizzate ad agevolare le stazioni appaltanti nel porre in essere gli adempimenti previsti dal Codice, hanno riguardato, in particolare, l'utilizzo della CEC-PAC (Comunicazione Elettronica Certificata – Pubblica Amministrazione Cittadino) e di caselle di posta ordinaria opportunamente configurate e con specifiche cautele di gestione che sostituiscano la Pec personale unicamente fino al termine del regime facoltativo di utilizzo del sistema AVCpass (previsto per il 31 dicembre 2013).

Il Garante ha inoltre verificato che l'AVCP, valutato quanto prescritto nel precedente parere del 19 dicembre 2012, n. 420 (doc. web n. 2171106), ha individuato il termine di sei mesi per la conservazione dei dati relativi agli accessi e alle operazioni compiute sul sistema AVCpass.

Accessi abusivi

Hanno altresì formato oggetto d'esame segnalazioni relative ad accessi abusivi al sistema informativo dell'Inps che, a seguito di accertamenti di carattere ispettivo svolti anche in collaborazione con il Nucleo della Guardia di finanza, hanno portato alla segnalazione dei fatti alle competenti Procure della Repubblica.

Gli estratti contributivi dei segnalanti erano stati acquisiti dal sistema informativo dell'Inps attraverso utenze regolarmente rilasciate dall'Istituto a soggetti, operanti presso patronati convenzionati, che avevano fatto accesso ai dati personali dei segnalanti in assenza della prescritta delega (note 15 e 22 ottobre 2013).

Inoltre, su segnalazione dell'Inps e di alcuni privati, l'Autorità ha collaborato con la Polizia postale in relazione ad un caso molto grave concernente innumerevoli accessi a banche dati pubbliche, compreso il sistema informativo dell'Istituto (nota 22 ottobre 2013). Al riguardo si è potuto presumere l'utilizzo illegittimo di credenziali assegnate ad operatori di patronato, riscontrando un elevato numero di connessioni al predetto sistema informativo originate da singoli indirizzi *Ip* con modalità di interrogazione compatibili con l'utilizzo di cd. robot per estrarre i dati. Le indagini di polizia giudiziaria, poste in essere dal Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic), hanno così permesso di porre fine ad un illecito servizio *online* realizzato utilizzando abusivamente le credenziali assegnate agli operatori di patronato per ricavare posizioni previdenziali e contributive. In particolare, una società è risultata offrire a pagamento tale servizio sul proprio sito web, a soggetti interessati all'accesso ad informazioni patrimoniali (in particolare, professionisti o società finanziarie), anche attraverso un sistema di ricariche prepagate.

Con riferimento, invece, ad una segnalazione relativa ad un presunto accesso abusivo all'Anagrafe tributaria, l'Ufficio ha richiesto all'Agenzia delle entrate di verificare eventuali accessi non autorizzati ai dati personali del segnalante. In seguito all'intervento dell'Autorità, l'Agenzia, dopo aver effettuato un'attività di tracciamento degli accessi avvenuti sui propri sistemi informativi, ha compiuto una complessa attività di *audit* all'esito della quale sono emerse condotte valutabili dal punto di vista penale che sono state comunicate, a cura della stessa Agenzia, alla Procura della Repubblica per le attività di competenza (nota 25 luglio 2013).

Anagrafe nazionale degli abilitati alla guida

Con provvedimento del 24 gennaio 2013, n. 25 (doc. web n. 2256617), del quale si è dato conto nella Relazione annuale 2012 (p. 73), il Garante aveva prescritto al Ministero delle infrastrutture e dei trasporti che, a partire dalla data del provvedimento, le comunicazioni agli interessati – anche nella forma della consultazione diretta tramite il cd. portale dell'automobilista – relative alle variazioni di punteggio della patente (decurtazioni e attribuzioni di punti) avrebbero dovuto contenere i dati relativi alla totalità delle variazioni dei punti della patente, ancor-

ché effettuate in modo automatizzato, ivi comprese l'attribuzione di punti che, successivamente, si rivelasse non legittimamente effettuata, in modo da rendere conoscibile all'interessato la relativa operazione di annullamento. Con riferimento agli eventi passati, il Garante aveva altresì prescritto che, su richiesta dell'interessato, avrebbe dovuto essere assicurata la conoscibilità, nel dettaglio e cronologicamente, dei dati concernenti la totalità delle variazioni di punteggio della patente.

In data 8 agosto 2013, il Ministero delle infrastrutture e dei trasporti ha fornito riscontro alle richieste formulate dal Garante nel citato provvedimento, comunicando di aver adeguato le procedure informatiche del sistema informativo per conformarsi alle sopramenzionate prescrizioni dell'Autorità.

4.3. *L'accesso ai documenti amministrativi*

Le tematiche riguardanti l'accesso ai documenti amministrativi continuano ad essere oggetto di intervento dell'Autorità a causa delle numerose segnalazioni e richieste di chiarimenti presentate sia dalle pp.aa., sia dai singoli. Tra le questioni più rilevanti, si registra il caso in cui il Garante ha riscontrato l'illiceità del trattamento dei dati personali effettuato in una Regione nella quale si è consentita la messa a disposizione e consultazione, da parte di alcuni dirigenti, del fascicolo personale di un dipendente – peraltro contenente dati idonei a rivelarne lo stato di salute – in violazione degli artt. 11, comma 1, lett. *d*), 20, commi 1 e 2, e 22, commi 3 e 5, del Codice (provv. 24 ottobre 2013, n. 469, doc. web n. 2799174).

L'Ufficio è stato nuovamente interessato da quesiti relativi alla possibilità di rendere ostensibile a testate giornalistiche documentazione in possesso dell'amministrazione. In particolare, il Servizio bilancio, contabilità, provveditorato ed assistenza al collegio dei revisori dei conti di un Consiglio regionale ha chiesto di pronunciarsi sulla istanza formulata da una testata giornalistica televisiva volta ad ottenere informazioni circa l'erogazione delle indennità a un consigliere regionale. In merito, è stato ribadito che il Codice non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (artt. 59 e 60) e che "i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla l. 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso" (art. 59, comma 1). Per tale motivo, le valutazioni relative alle determinazioni assunte dall'amministrazione interpellata aventi ad oggetto le richieste di accesso ai documenti esulano dall'ambito di competenza del Garante e rimangono sindacabili di fronte alle autorità competenti (art. 25, l. n. 241/1990).

In ordine, poi, alle eventuali richieste di accesso formulate dagli organi di stampa, la disciplina in materia di protezione dei dati personali – non avendo inciso in modo restrittivo sulla normativa posta a salvaguardia della trasparenza amministrativa – non può essere invocata per negare, in via di principio, l'accesso ai documenti. Di conseguenza, rimane "affidata alla responsabilità del giornalista l'utilizzazione lecita del dato raccolto e quindi la sua diffusione secondo i parametri dell'essenzialità rispetto al fatto d'interesse pubblico narrato, della correttezza, della pertinenza e della non eccedenza, avuto altresì riguardo alla natura del dato medesimo". Tale indicazione – contenuta già nei chiarimenti del Garante del 6 maggio 2004 (doc. web n. 1007634) – è rivolta a chi, nell'esercizio dell'attività giornalistica, utilizza la documentazione a cui ha avuto legittimamente accesso e costituisce un'applicazione dei principi generali già dettati

dal Codice (cfr. in particolare l'art. 137) nonché dalle disposizioni del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (Allegato A.1 al Codice) (nota 23 settembre 2013).

Accesso dei consiglieri regionali

Sul bilanciamento tra il diritto dei consiglieri regionali ad accedere alle informazioni utili all'espletamento del loro mandato e il diritto alla riservatezza, in particolare quando la richiesta di accesso riguarda documentazione sanitaria riferita a terze persone, è intervenuto il Garante a seguito delle segnalazioni di due amministrazioni regionali destinatarie di istanze di accesso a certificati medici e cartelle cliniche per verificare la correttezza dei servizi erogati dagli organi sanitari regionali (provv. 25 luglio 2013, n. 369, doc. web n. 2536172).

Nel primo caso, il Presidente di un Consiglio regionale aveva chiesto di conoscere i nominativi del personale medico e infermieristico giudicato inabile a svolgere alcune mansioni presso Asl, aziende e presidi ospedalieri del Servizio sanitario regionale nonché di visionare le copie delle certificazioni di invalidità e di verificare la composizione degli organi di accertamento dello stato invalidante. Nel secondo caso, un consigliere regionale aveva formulato istanza di accesso ad una Asl con riguardo alla cartella clinica di un paziente sottoposto a trattamento sanitario obbligatorio (Tso) per effettuare delle verifiche.

A tale proposito, il Garante ha richiamato la disciplina sul trattamento di dati sensibili effettuato da soggetti pubblici, che considera di rilevante interesse pubblico il trattamento delle sole informazioni indispensabili per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo, quale, appunto, quello dei consiglieri regionali (art. 65, comma 4, lett. *b*), del Codice).

Su tale base, l'Autorità ha sottolineato come il diritto di accesso a dati sensibili da parte dei consiglieri regionali incontri un limite nel rispetto dei principi di indispensabilità e di diretta riconducibilità alla funzione perseguita (artt. 20 e 22 del Codice), precisando che l'osservanza di tali principi deve essere particolarmente accurato quando l'istanza ha ad oggetto, come nei casi segnalati, documentazione sanitaria, riferita a persone identificate o identificabili, in relazione alla quale l'ordinamento prevede un particolare regime di tutela, oltre ai comuni obblighi di rispetto del segreto professionale del medico.

La protezione dei dati di carattere personale, con particolare riferimento a quelli attinenti alla salute, gioca infatti un ruolo fondamentale per l'esercizio del diritto al rispetto della vita privata e familiare garantito dall'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Come ha rilevato la Corte europea dei diritti dell'uomo, il rispetto del carattere confidenziale delle informazioni idonee a rivelare lo stato di salute costituisce un principio essenziale del sistema giuridico di tutti i Paesi europei aderenti alla Convenzione; ciò non soltanto al fine di proteggere la vita privata dei pazienti, ma anche di salvaguardare la fiducia generale nei confronti del personale medico e dei servizi sanitari in generale (cfr. Corte EDU, *Z v. Finland*, sentenza 25 febbraio 1997).

Pertanto, seppure tra i compiti affidati all'Autorità non rientra quello di autorizzare o negare l'accesso ai documenti amministrativi, il Garante ha ritenuto opportuno precisare, in relazione alle peculiari vicende prospettate, che le richieste avanzate dai consiglieri regionali possono essere soddisfatte attraverso modalità che assicurino che l'esercizio delle attività di controllo nell'espletamento del mandato del consigliere avvenga, in concreto, in modo da comportare il minor pregiudizio possibile alla vita privata delle persone interessate. Ciò anche al fine di garantire che il diritto di accesso sia esercitato con riguardo ai dati effettivamente utili per l'esercizio del mandato e ai fini di questo, fermo restando che i dati personali eventualmente acquisiti dal consigliere possono essere utilizzati per le sole finalità pertinenti al mandato.

Tornando quindi ai casi sopra richiamati, nel primo l'Autorità ha prescritto che il Presidente del Consiglio regionale possa accedere alle informazioni richieste solo previo oscuramento dei nominativi del personale giudicato inabile a svolgere alcune mansioni. Nel secondo, il Garante ha disposto che il consigliere regionale istante possa accedere alla cartella clinica del paziente sottoposto a Tso solo dopo avere interpellato la persona interessata (o il suo legale rappresentante) al fine di consentire all'interessato di opporsi per motivi legittimi al trattamento di informazioni che lo riguardano (art. 7, comma 4, del Codice).

Sulle misure prescritte alle due Regioni il Garante ha ritenuto opportuno acquisire il previo parere della Commissione per l'accesso ai documenti amministrativi presso la Presidenza del Consiglio dei Ministri.

Anche le problematiche riguardanti l'accesso di consiglieri comunali agli atti degli enti locali di appartenenza sono state sottoposte all'attenzione dell'Autorità da una società trasporto passeggeri e da un comune. Sul punto è stato ricordato che il Garante ha sempre evidenziato la piena vigenza della specifica disposizione di legge che riconosce ai consiglieri comunali e provinciali il "diritto di ottenere dagli uffici, rispettivamente, del comune e della provincia, nonché dalle loro aziende ed enti dipendenti, tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato" (art. 43, comma 2, d.lgs. 18 agosto 2000, n. 267). Anche in tal caso, la disciplina di riferimento demanda al soggetto interpellato – che non deve chiedere alcun consenso agli interessati (artt. 24, comma 1, lett. *a*), del Codice), né alcuna autorizzazione all'Autorità – l'obbligo di accertare l'ampia e qualificata posizione di pretesa all'informazione *ratione officii* dei consiglieri degli enti locali interessati, nel rispetto dei limiti e delle condizioni stabilite dalla richiamata normativa di settore (art. 43, comma 2, d.lgs. n. 267/2000) (note 28 maggio e 5 novembre 2013).

4.4. *La trasparenza amministrativa*

Per quanto riguarda il tema della trasparenza e della pubblicazione su internet di informazioni personali sono pervenute numerose istanze in ordine al corretto trattamento dei dati personali contenuti in atti e delibere diffusi sui siti web di organi istituzionali statali nonché di regioni ed enti locali.

In proposito il Garante aveva già adottato le "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" (provv. 2 marzo 2011, n. 88, doc. web n. 1793203). Tali linee guida – attualmente in fase di revisione e aggiornamento a seguito dell'entrata in vigore del d.lgs. 14 marzo 2013, n. 33, in relazione al quale il Garante ha, come detto, reso un proprio parere (provv. 7 febbraio 2013, n. 49, doc. web n. 2243168, sul quale v. *supra* par. 3.2.2) – individuavano un primo quadro unitario di misure e accorgimenti destinati a tutte le pp.aa. che effettuano, in attuazione alle disposizioni normative vigenti, attività di comunicazione o diffusione di dati personali sui propri siti istituzionali per finalità di trasparenza, pubblicità dell'azione amministrativa, nonché di consultazione di atti su iniziativa di singoli.

Diffusione di dati relativi a Tso

Sul tema, si evidenzia la condotta, tenuta da 27 comuni e segnalata dalla Guardia di finanza, consistente nella pubblicazione delle ordinanze del sindaco sui siti istituzionali nelle quali, riportando in chiaro i dati identificativi e la patologia sofferta dai soggetti sottoposti a trattamento sanitario obbligatorio (Tso) (ed in molti casi indicizzando i predetti dati nei principali motori di ricerca generalisti), si autorizzavano i menzionati trattamenti sanitari. In tali fattispecie è stato rilevato che l'art. 22, comma

8, del Codice prevede che nel trattamento effettuato da soggetti pubblici i "dati idonei a rivelare lo stato di salute non possono essere diffusi" (cfr., in tal senso, anche l'art. 65, comma 5, e l'art. 68, comma 3, del Codice) e che, pertanto, è vietata la diffusione di dati da cui si possa desumere 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. Per questa ragione, è stata vietata l'ulteriore diffusione su internet di tali dati prescrivendo ai comuni di attivarsi presso i responsabili dei principali motori di ricerca, al fine di sollecitare la rimozione delle copie web delle ordinanze di Tso dagli indici e dalla *cache* dei motori di ricerca [cfr. provv.ti 3 ottobre 2013, n. 432 (doc. web n. 2747962); 4 aprile 2013, n. 160 (doc. web n. 2488234), n. 159 (doc. web n. 2473879), n. 158 (doc. web n. 2460997), n. 157 (doc. web n. 2452536), n. 156 (doc. web n. 2448446), n. 155 (doc. web n. 2433468), n. 154 (doc. web n. 2427771); 21 marzo 2013, n. 140 (doc. web n. 2389232), n. 137 (doc. web n. 2390451), n. 139 (doc. web n. 2390632), n. 138 (doc. web n. 2390488); 14 marzo 2013, n. 121 (doc. web n. 2389148), n. 120 (doc. web n. 2388972), n. 119 (doc. web n. 2388608), n. 118 (doc. web n. 2388550), n. 117 (doc. web n. 2388358); 7 marzo 2013, n. 102 (doc. web n. 2352966), n. 101 (doc. web n. 2350940), n. 100 (doc. web n. 2343470), n. 99 (doc. web n. 2324649), n. 98 (doc. web n. 2324625), n. 97 (doc. web n. 2322279), n. 96 (doc. web n. 2322248), n. 95 (doc. web n. 2322211), n. 94 (doc. web n. 2322055), n. 93 (doc. web n. 2322036); 21 febbraio 2013, n. 76 (doc. web n. 2358792), n. 75 (doc. web n. 2355041)].

Analogo provvedimento è stato adottato nei confronti di un comune (provv. 3 ottobre 2013, n. 432, doc. web n. 2747962) che aveva pubblicato una determinazione dirigenziale avente ad oggetto la concessione di un beneficio economico a un malato, indicando in chiaro la patologia nonché i dati anagrafici (nominativo, luogo e data di nascita) dell'interessato e del proprio "familiare referente" (comprensivi del codice fiscale e del numero Iban su cui accreditare le somme). Anche in questa circostanza, è stato rilevato che i soggetti pubblici non possono diffondere dati idonei a rivelare lo stato di salute (artt. 22, comma 8, 65, comma 5 e 68, comma 3, del Codice), vietando, come nel caso precedente, l'ulteriore diffusione dei dati sul web e prescrivendo la rimozione della copia web della predetta determinazione dirigenziale dagli indici nonché dalla *cache* dei motori di ricerca.

Sempre in materia di trasparenza, si segnalano alcuni interventi funzionali a richiamare l'attenzione sulla necessità che la diffusione di dati personali sia sempre prevista da idonei presupposti normativi. Si richiamano, a titolo esemplificativo, le segnalazioni ricevute in ordine al trattamento effettuato da due comuni che hanno proceduto alla pubblicazione dei dati dei bambini ammessi (e non) al servizio di trasporto scolastico, con indicazione del nominativo di ciascuno e di ulteriori informazioni (quali il codice fiscale, il numero di linea del mezzo utilizzato, l'orario di partenza e di ritorno), lasciando peraltro che i nominativi fossero indicizzabili dai motori di ricerca. L'Ufficio ha ritenuto tali condotte non conformi al Codice attesa l'assenza di idonei presupposti normativi per la diffusione (art. 19, comma 3, del Codice) (note 10 aprile e 21 novembre 2013).

Albo pretorio *online*

Continuano a pervenire segnalazioni relative alla diffusione di dati personali sull'albo pretorio *online* degli enti locali o di altri soggetti pubblici rispetto alle quali si è più volte riscontrata una condotta non conforme alla disciplina in materia di dati personali per la mancanza di un idoneo presupposto normativo per la pubblicazione oppure in ragione della persistente diffusione dei dati personali sul web oltre il periodo previsto per l'affissione all'albo (ad es., quindici giorni per l'albo pretorio; cfr. artt. 19, comma 3, del Codice e 124, d.lgs. 18 agosto 2000, n. 267) (note 5 gennaio e 19 aprile 2013).

Sanzioni amministrative su siti istituzionali

Si segnalano inoltre alcuni interventi sulla questione della pubblicazione sui siti web istituzionali dei comuni dei nomi dei soggetti destinatari di sanzioni amministrative. Al riguardo, l'Ufficio ha ritenuto che la pubblicazione dei dati personali degli autori di illeciti amministrativi costituisca una sanzione accessoria che, in quanto tale, può essere prevista solo da una legge. In base alla normativa di settore e come ribadito dalla costante giurisprudenza di legittimità, infatti, anche per le sanzioni amministrative accessorie è necessario rispettare il principio di legalità alla luce del quale "nessuno può essere assoggettato a sanzioni amministrative se non in forza di una legge che sia entrata in vigore prima della commissione della violazione" (art. 1, comma 1, l. 24 novembre 1981 n. 689; cfr., *ex plurimis*, Corte cost. 5 aprile 2012, n. 82) (nota 24 aprile 2013).

Sulla medesima questione è stata ritenuta illecita la pubblicazione sul sito web istituzionale di un comune dei verbali di violazione del codice della strada contenenti dati personali, in quanto priva di un idoneo presupposto normativo (art. 19, comma 3, del Codice) (nota 22 luglio 2013).

4.5. *La documentazione anagrafica e la materia elettorale*

Nel periodo di riferimento, la materia anagrafica ed elettorale è stata oggetto di attenzione da parte dell'Autorità.

Liste elettorali

Nel caso di una richiesta di chiarimenti da parte di alcuni comuni in ordine alla legittimità del rilascio di copia delle liste elettorali ad associazioni (anche onlus), l'Ufficio ha precisato che la normativa di settore ammette il rilascio di elenchi degli iscritti nell'Anagrafe della popolazione residente solamente verso le pp.aa. "che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità", mentre il rilascio di dati anagrafici a privati può essere disposto dall'ufficiale di anagrafe solo se si tratta di dati "resi anonimi e aggregati" e per "fini statistici e di ricerca" (art. 34, commi 1 e 2, d.P.R. 30 maggio 1989 n. 223). A tali comuni è stata pertanto richiamata la normativa di settore che, invece, prevede che le "liste elettorali possono essere rilasciate in copia per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso" (art. 177, comma 5, del Codice, che ha sostituito l'art. 51, comma 5, d.P.R. 20 marzo 1967, n. 223) (note 29 aprile e 28 maggio 2013).

Elenchi anagrafici

Un altro caso ha riguardato la richiesta, formulata da un dipartimento di sanità pubblica del Servizio sanitario regionale, volta ad acquisire elenchi e vari dati anagrafici relativi a cittadini residenti in 74 comuni della regione, allo scopo di realizzare un progetto volto a migliorare le conoscenze relative agli aspetti ambientali e a valutarne l'impatto sulla salute dei cittadini (Progetto "Supersito" – Regione Emilia Romagna). A mente di quanto previsto dall'art. 19, comma 2, del Codice, l'Ufficio ha richiamato la disciplina di settore che prevede il rilascio alle pp.aa. di elenchi di iscritti all'Anagrafe "per esclusivo uso di pubblica utilità", nonché di dati "resi anonimi ed aggregati, agli interessati che ne facciano richiesta per fini statistici e di ricerca" (art. 34, comma 1, d.P.R. 30 maggio 1989, n. 223); è inoltre previsto il rilascio di "dari anagrafici, resi anonimi ed aggregati, agli interessati che ne facciano richiesta per fini statistici e di ricerca" (art. 34, comma 1, d.P.R. 30 maggio 1989, n. 223). Nel caso di specie, il Garante ha precisato che i trattamenti che il Dipartimento di sanità pubblica del Servizio sanitario regionale, in collaborazione con l'Agenzia regionale per la protezione ambientale (Arpa), andava ad effettuare, ove finalizzati alla ricerca scientifica in campo medico, bio-

medico o epidemiologico (in particolare, con dati già raccolti presso strutture sanitarie o esercenti le professioni sanitarie per fini di cura della salute o per l'esecuzione di precedenti progetti di ricerca) avrebbero dovuto essere conformi alle specifiche disposizioni sulla ricerca scientifica in campo medico, biomedico ed epidemiologico (artt. 106 e 110 del Codice; Allegato A.4, codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, doc. web n. 1556635; autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica, del 1° marzo 2012, n. 85, doc. web n. 1878276). Ove, invece, i medesimi trattamenti fossero preordinati al perseguimento di finalità amministrative correlate ai compiti del Servizio sanitario, avrebbe dovuto essere rispettato il quadro generale di garanzie previsto dalla legislazione in materia di trattamento di dati sensibili e dallo specifico regolamento regionale adottato in conformità allo schema tipo (sul quale il Garante ha espresso parere favorevole con provvedimento del 13 aprile 2006, doc. web n. 1272225) (nota 17 dicembre 2013).

Certificati *online*

Si segnala altresì il caso di un cittadino che aveva lamentato l'attivazione, sul sito web istituzionale del proprio comune di residenza, del servizio *online* attraverso il quale era possibile scaricare certificati (fra gli altri, di residenza, cittadinanza, nascita, esistenza in vita, stato civile, godimento dei diritti politici, iscrizione nelle liste elettorali, matrimonio, stato di famiglia) senza alcun tipo di autenticazione o accesso selezionato, ma inserendo semplicemente il codice fiscale dell'interessato. L'Ufficio ha richiesto informazioni al Dipartimento per gli affari interni e territoriali presso il Ministero dell'interno, il quale ha evidenziato, tra l'altro, che l'Agenzia per l'Italia Digitale, interpellata al riguardo, si era espressa nel senso che, ai sensi dell'art. 64, d.lgs. 7 marzo 2005, n. 82 (Cad), ai fini dell'identificazione *online*, l'inserimento del solo codice fiscale non rientra tra gli "strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi" (*ex* comma 2 dell'art. 64 cit.) utili all'individuazione del soggetto richiedente il servizio. È stato inoltre rappresentato che la soluzione tecnologica "timbro digitale" per l'autenticazione delle certificazioni anagrafiche e di stato civile, autorizzata dallo stesso Ministero dell'interno in via sperimentale in alcuni comuni, prevede che la richiesta, da parte del cittadino, della certificazione avvenga previa autenticazione informatica e riconoscimento "con CIE/CBNS e *user id-password* per i servizi richiesti da web". In tale quadro, pertanto, il comune in questione è stato invitato a voler tenere in considerazione le corrette modalità, così individuate, per consentire l'accesso ai predetti certificati in conformità alla disciplina di settore (nota 5 luglio 2013).

Anagrafe elettorale

In tema di anagrafe elettorale dei soggetti residenti all'estero l'Ufficio è intervenuto per fornire informazioni in merito alla cancellazione di un nominativo dalle liste elettorali della circoscrizione consolare estera di residenza. In proposito, è stato rappresentato che la normativa di settore stabilisce che "sono iscritti di ufficio nelle liste elettorali i cittadini che, possedendo i requisiti per essere elettori e non essendo incorsi nella perdita definitiva o temporanea del diritto elettorale attivo, sono compresi nell'Anagrafe della popolazione residente nel comune o nell'Anagrafe degli italiani residenti all'estero (Aire)" (art. 4, d.P.R. 20 marzo 1967, n. 223) e che "sono elettori tutti i cittadini italiani che abbiano compiuto il diciottesimo anno di età" salvo eccezioni previste dalla legge (cfr., in particolare, artt. 1 e 2 del decreto citato); disposizioni normative puntuali disciplinano espressamente, inoltre, le ipotesi di rettifica e revisione delle liste elettorali (cfr., in particolare, artt. 20 e 32 del decreto citato). È stato pertanto chiarito che, al di fuori delle ipotesi che la normativa di settore ha preso in considerazione, non è possibile ottenere la cancellazione del proprio nominativo dalle liste elettorali (nota 10 settembre 2013).

Aire

Analogamente, con riferimento alla segnalazione di un cittadino relativa alla ricezione di un messaggio di propaganda elettorale al proprio indirizzo di residenza all'estero, è stato evidenziato che, già con il provvedimento del 7 settembre 2005 (doc. web n. 1165613) – richiamato dal provvedimento del 10 gennaio 2013, n. 1 (doc. web n. 2181429) –, per attività di propaganda elettorale sono utilizzabili senza consenso i dati contenuti "nelle liste elettorali che ciascun comune tiene, aggiorna costantemente e rilascia in copia anche su supporto elettronico" nonché l'"elenco aggiornato dei cittadini italiani residenti all'estero finalizzato a predisporre le liste elettorali, realizzato unificando i dati dell'anagrafe degli italiani residenti all'estero (Aire) e degli schedari consolari". In merito, la specifica normativa di settore prevede che "Il Governo, mediante unificazione dei dati dell'anagrafe degli italiani residenti all'estero e degli schedari consolari, provvede a realizzare l'elenco aggiornato dei cittadini italiani residenti all'estero finalizzato alla predisposizione delle lisre elettorali" (art. 5, comma 1, l. n. 459/2001) e che nell'elenco aggiornato dei cittadini italiani residenti all'estero di cui all'art. 5, comma 1, l. n. 459/2001, "sono registrati i seguenti dati: nome e cognome del cittadino italiano, cognome del coniuge per le donne coniugate o vedove, luogo e data di nascita, sesso, stato di residenza, inditizzo, casella postale, ufficio consolare, comune di isctizione all'anagrafe degli italiani residenti all'estero" (art. 5, comma 1, d.P.R. 2 aprile 2003, n. 104). La medesima normativa prevede altresì che "dopo la realizzazione dell'elenco aggiornato con le modalità di cui al presente articolo, il Ministero dell'interno comunica in via informatica al Ministero degli affari esteri, entro il sessantesimo giorno antecedente la data delle votazioni in Italia, l'elenco provvisorio dei residenti all'estero aventi diritto al voto, ai fini della successiva distribuzione in via informatica agli uffici consolari per gli adempimenti previsti dalla legge" (art. 5, comma 8, d.P.R. n. 104/2003). Alla luce di tali elementi, non sono stati ravvisati gli estremi per promuovere l'adozione di un provvedimento del Garante (nota 29 maggio 2013).

Sotto un diverso profilo, il Dipartimento per gli affari interni e territoriali presso il Ministero dell'interno (nota 31 maggio 2013) ha informato l'Autorità di aver pienamente aderito all'orientamento da questa espresso (nota 29 agosto 2012, in Relazione 2012, p. 77) in ordine ad una richiesta presentata da Ancitel s.p.a. di ottenere copia delle liste elettorali in qualità di responsabile del trattamento designata da taluni enti *non profit*, che agiscono quali titolari del trattamento per finalità comprese tra quelle previste dalle vigenti disposizioni in materia (art. 51, comma 5, d.P.R. n. 223/1967, come modificato dall'art. 177, comma 5, del Codice). Nella richiesta era previsto che i predetti dati sarebbero stati successivamente trasmessi per l'elaborazione a Consodata s.p.a., anch'essa designata responsabile e da questa consegnati ai suddetti enti. A tal proposito è stato rappresentato dall'Ufficio che le organizzazioni non lucrative, legittimate ad ottenere dai comuni il rilascio di copia delle liste elettorali e ad utilizzarle per il perseguimento delle finalità individuate dalla normativa vigente, possono richiedere a soggetti esterni (nel caso di specie Ancitel s.p.a. e Consodata s.p.a.) lo svolgimento di specifiche operazioni di trattamento. I dati, però, non possono essere comunicati ad altri titolari e possono essere utilizzati solo per le finalità perseguite dagli enti titolari del trattamento riconducibili a quelle tassativamente individuate dal citato art. 51, comma 5, d.P.R. n. 223/1967.

In prossimità delle consultazioni elettorali tenute nel mese di febbraio 2013 per le elezioni dei consigli regionali delle Regioni Lombardia e Molise nonché per le consultazioni tenute a maggio per le elezioni dei sindaci, dei consigli comunali nonché dei consigli circoscrizionali, e per le consultazioni tenute nel mese di giugno per l'elezione del Presidente e del Consiglio regionale della Regione Autonoma Valle d'Aosta, l'Autorità ha approvato alcuni provvedimenti (provv.ti 10 gennaio 2013,

n. 1, doc. web n. 2181429; 24 aprile 2013, n. 228, doc. web n. 2404305) che confermano le prescrizioni già stabilite dal provvedimento generale del 7 settembre 2005 (doc. web n. 1165613), prevedendo speciali casi di esonero temporaneo dall'informativa per partiti, movimenti politici, sostenitori e singoli candidati in relazione all'uso dei dati personali a fini di comunicazione politica e di propaganda elettorale. Il citato provvedimento del 24 aprile 2013, n. 228, ha ribadito che i cittadini devono essere sempre informati sull'uso effettuato dei loro dati. Tuttavia, partiti, movimenti politici, sostenitori e singoli candidati sono stati esonerati dal predetto obbligo di informativa sino al 31 agosto 2013 solo per i dati raccolti da registri ed elenchi pubblici, e utilizzati per l'invio di materiale propagandistico di dimensioni così ridotte da non consentire di inserirvi una informativa, anche sintetica. Trascorso tale termine il Garante ha altresì previsto che i medesimi soggetti devono fornire agli interessati un'idonea informativa entro il 31 ottobre 2013 o altrimenti cancellare le informazioni personali. È stato altresì rappresentato che, alla luce del quadro normativo successivo alle modifiche all'art. 130 del Codice e della istituzione del "Registro pubblico delle opposizioni" (art. 13, comma 3, del Codice; d.P.R. 7 settembre 2010, n. 178), per i trattamenti effettuati per l'inoltro di messaggi elettorali e politici è necessario il consenso informato degli intestatari di utenze pubblicate negli elenchi telefonici; è stata inoltre ribadita la necessità del consenso degli interessati per talune modalità di comunicazione (in particolare per l'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore, nonché mediante dispositivi quali, ad es., posta elettronica, telefax, messaggi del tipo mms o sms), come previsto dall'art. 130, commi 1 e 2, del Codice.

4.6. *L'istruzione scolastica ed universitaria*

Anche nel 2013 l'Autorità è intervenuta fornendo chiarimenti in relazione al trattamento di dati personali effettuato nell'ambito dell'istruzione scolastica ed universitaria.

In particolare, una scuola ha posto un quesito circa la necessità di acquisire la preventiva autorizzazione del Garante al fine di poter istituire un "ambiente di apprendimento" *online* con servizi disponibili per gli studenti. Al riguardo, l'Ufficio, nel precisare che, salvo i casi espressamente previsti, i trattamenti di dati personali non devono essere previamente autorizzati dal Garante, ha ribadito il dovere di rispettare la disciplina in materia di protezione dei dati personali, evidenziando, in particolare, la necessità di sottoporre a verifica preliminare i trattamenti che presentano specifici rischi per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che possono determinare (artt. 17, 40 e 41 del Codice; nota 25 giugno 2013).

È stata segnalata una presunta violazione della disciplina in materia di dati personali presso una scuola superiore di secondo grado in relazione alla somministrazione agli alunni di un test nominativo riguardante una ricerca promossa dal Dipartimento di psicologia dell'Università di Firenze, effettuata senza fornire preventivamente l'informativa sul trattamento dei dati personali (art. 13 del Codice). A seguito dell'intervento dell'Ufficio, il dirigente scolastico ha garantito di aver proceduto alla distruzione dei test compilati dagli studenti, dopo averli messi in sicurezza al fine di impedirne l'accesso a chiunque (ivi compresi i ricercatori dell'Università), e di aver successivamente consentito la somministrazione del test solo dopo che fosse stata fornita idonea informativa agli studenti. Considerate le garanzie e le idonee assicurazioni fornite, volte ad evitare la ripetizione per il futuro della condotta lamentata, e salva la veri-

fica dei presupposti per la contestazione di eventuali sanzioni amministrative, non sono state intraprese iniziative per l'adozione di provvedimenti da parte del Garante (nota 30 maggio 2013).

È giunta all'Autorità una segnalazione con la quale veniva rappresentato che, ai fini dell'iscrizione all'asilo nido di un comune, venivano raccolti dati personali ritenuti eccedenti e non pertinenti. In particolare, attraverso la modulistica predisposta per l'iscrizione, si richiedeva una pluralità di informazioni inerenti: "il motivo di assenza di uno dei genitori dal nucleo familiare, la presenza di un procedimento di affido o adozione in corso, l'origine straniera di uno o entrambi i genitori, con l'indicazione dell'anno di ingresso in Italia, la professione o la scuola frequentata da altri figli componenti il nucleo familiare, il nome, il cognome, la data di nascita, la residenza dei nonni del minore e se risultano residenti nel territorio del comune, anche l'occupazione, ivi compreso l'orario settimanale di lavoro, lo stato di salute e l'invalidità". L'Ufficio ha potuto accertare che, in base al regolamento comunale, le domande per l'iscrizione all'asilo nido contenenti le informazioni richieste relative alle "situazioni particolari che caratterizzano il nucleo familiare" concernevano esclusivamente la presenza di uno o più componenti con invalidità certificata ai sensi della legislazione vigente, superiore al 67% nonché del nucleo familiare in situazione di fragilità in carico ai servizi sociali. Su tali basi, rilevato il disallineamento tra la più ampia rosa di dati personali richiesti dal comune e quelli effettivamente necessari per verificare la sussistenza dei requisiti di ammissione all'asilo nido, il Garante ha ritenuto indebita l'acquisizione dei dati personali eccedenti. L'Autorità ha, pertanto, vietato al comune la raccolta ed il successivo trattamento dei predetti dati personali nonché di ogni altra informazione non rilevante ai fini della verifica dei criteri previsti nel regolamento comunale, in quanto ciò avrebbe comportato un trattamento di dati personali eccedenti, non pertinenti e, con specifico riferimento ai dati sensibili, non indispensabili rispetto alle finalità perseguite (provv. 6 giugno 2013, n. 273, doc. web n. 2554925).

Comunicazione ai sensi dell'art. 39 del Codice

Una provincia aveva richiesto, ai sensi dell'art. 39 del Codice, al Ministero dell'istruzione, dell'università e della ricerca i dati relativi ai codici fiscali degli studenti della scuola secondaria della provincia "frequentanti, trasferiti, ritirati, bocciati, *etc.*, del primo e ultimo anno di corso, con riferimento agli anni 2012/2013 e 2013/2014", per lo svolgimento delle proprie funzioni istituzionali inerenti la vigilanza sull'assolvimento dell'obbligo scolastico e la realizzazione di un progetto di contrasto alla dispersione scolastica (art. 68, l. 17 maggio 1999, n. 144 e D.G.R. 1891 del 22 giugno 2011). Sul punto l'Ufficio ha preliminarmente evidenziato che il Codice dispone, in via generale, che i soggetti pubblici possano comunicare dati personali, diversi da quelli sensibili e giudiziari, solo se tale specifica operazione di trattamento sia prevista da una norma di legge o di regolamento (cfr. art. 19, comma 3). Inoltre, come ipotesi residuale, in mancanza di una specifica norma di legge o di regolamento che lo preveda, le amministrazioni pubbliche possono comunicare ad altri soggetti pubblici dati personali, non aventi natura sensibile, allorquando tale trattamento sia necessario per lo svolgimento delle proprie funzioni istituzionali. Le amministrazioni coinvolte nel flusso di dati che si intende attivare devono, pertanto, preliminarmente ed attentamente accertare che tale flusso di dati non sia già previsto dalla specifica normativa di settore. In tal caso, il titolare è tenuto ad effettuare una comunicazione preventiva al Garante e il trattamento potrà avere inizio decorsi quarantacinque giorni della predetta comunicazione, salva diversa determinazione anche successiva dell'Autorità (artt. 18, comma 2, 19, comma 2 e 39 del Codice). Su tali basi, rilevata la sussistenza di specifiche disposizioni di regolamento che espressamente disciplinano il flusso di dati necessari alla provincia per l'assolvimento delle funzioni istituzionali concernenti l'obbligo di frequenza di attività formative fino al diciottesimo anno di età e di preven-

zione e contrasto alla dispersione scolastica, l'Ufficio ha ritenuto che le comunicazioni di dati personali per le predette finalità possano avvenire solo nei limiti previsti dalla disciplina di settore (art. 3, commi 2, 3, 4, e 5, e art. 8, comma 2, d.P.R. 12 luglio 2000, n. 257; art. 3, comma 2, d.m. 5 agosto 2010, n. 74 e punto 3 sezione "profilo D" dell'allegato tecnico al d.m. n. 74/2010 cit.) (nota 27 febbraio 2013).

Similmente, il Ministero dell'istruzione, dell'università e della ricerca (Miur) ha comunicato all'Autorità, ai sensi degli artt. 19, comma 2 e 39, comma 2, del Codice, di aver ricevuto da parte di un comune la richiesta dei dati relativi agli alunni iscritti dal 2007 alle scuole di ogni ordine e grado della provincia di appartenenza (nome, cognome, data e luogo di nascita, scuola frequentata ed anno di frequenza) per il perseguimento della funzione istituzionale di partecipazione al contrasto all'evasione fiscale, con particolare riferimento all'accertamento delle residenze fittizie all'estero attraverso la vigilanza sui soggetti che hanno richiesto l'iscrizione all'Aire (in particolare, art. 44, d.P.R. 29 settembre 1973, n. 600 e ss. mm. e art. 83, commi 16 e 17, d. l. 25 giugno 2008, n. 112, convertito dalla l. 6 agosto 2008, n. 133 e ss. mm.).

Al riguardo, l'Ufficio ha rilevato che la normativa di settore stabilisce specifiche regole per il reperimento da parte dei comuni delle informazioni necessarie per la partecipazione al contrasto all'evasione fiscale (cfr. art. 1, d.l. 30 settembre 2005, n. 203 convertito, con modificazioni, dalla l. 2 dicembre 2005, n. 248 e modificato dall'art. 18, d.l. 31 maggio 2010, n. 78, convertito dalla l. 30 luglio 2010, n. 122; provvedimenti del Direttore dell'Agenzia delle entrate del 3 dicembre 2007 e del 26 novembre 2008; art. 44, d.P.R. n. 600/1973; art. 83, commi 16 e 17, d.l. n. 112/2008). Tenuto conto della citata normativa, l'Ufficio ha ritenuto quindi non applicabile la disciplina prevista dagli artt. 19, comma 2 e 39, comma 2, del Codice (cfr. in particolare, i citati artt. 44, d.P.R. n. 600/1973 e 83, d.l. n. 112/2008) (nota 21 maggio 2013).

Relativamente al settore universitario, una studentessa ha segnalato all'Autorità che, presso l'Università degli Studi di Roma la Sapienza, attraverso un sistema informatico, ogni docente, inserendo le proprie credenziali, poteva visionare i dati personali di qualunque studente iscritto. L'Università, nel confermare il contenuto della segnalazione, ha messo a punto specifiche soluzioni operative in base alle quali, in particolare, "a partire dall'anno accademico 2013/2014, tutte le carriere degli studenti iscritti ai corsi [...] porranno essere visualizzate da docente sul predetto sistema informatico [...] solo ed esclusivamente nel caso che lo studente si sia già iscritto a sostenere l'esame di profitto di competenza; relativamente alle carriere, ad esaurimento, dei vecchi ordinamenti, per le quali non sono attivi filtri automarici di controllo sul piano di studio, è possibile sviluppare una nuova funzione del sistema [...] che consenta allo studente di autorizzare l'accesso ai propri dati di carriera ai docenti con i quali intenda sostenere esami di profitto; in tal modo ogni docente potrà accedere esclusivamente alle carriere che sono di pertinenza della propria attività istituzionale". Sulla base di tali specifiche assicurazioni l'Ufficio, salva la verifica dei presupposti per la contestazione di eventuali sanzioni amministrative, non ha promosso l'adozione di specifici provvedimenti da parte del Garante (nota 5 aprile 2013).

4.7. *L'attività fiscale e tributaria*

Redditometro

L'Agenzia ha richiesto al Garante una verifica preliminare sul trattamento di dati personali che intendeva effettuare ai fini dell'accertamento sintetico del reddito delle persone fisiche di cui all'art. 38, commi 4 e 5, d.P.R. 29 settembre 1973, n. 600 (il nuovo cd. redditometro), modificato dall'art. 22, d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122.

Il nuovo strumento di accertamento sintetico è stato sottoposto alla verifica preliminare del Garante perché il calcolo dello scostamento tra i redditi dichiarati e le spese effettuate, utilizzato per selezionare i contribuenti da sottoporre a controlli, è fondato:

- sul trattamento automatizzato di dati personali presenti in Anagrafe tributaria, o comunque conosciuti dall'Agenzia, al fine di selezionare i contribuenti da sottoporre ad accertamento e rideterminarne il reddito sulla base di informazioni comunicate dallo stesso contribuente in ragione di obblighi dichiarativi (ad es., dichiarazione dei redditi, atti del registro) o da soggetti esterni in base ad un obbligo di legge (ad es., operatori telefonici, assicurazioni), nonché altrimenti ricavate dall'Agenzia nell'ambito di specifiche campagne di controllo (ad es., presso *tour operator*, scuole private, *etc.*);
- sull'imputazione al contribuente di spese presunte, quantificate sulla base dell'attribuzione di un profilo (*cluster*) ricavato anche ricorrendo alle ccdd. "spese medie Istat", in relazione alla sua appartenenza ad una specifica tipologia di famiglia e alla residenza in una determinata area geografica.

L'individuazione di criteri astratti volti ad analizzare il comportamento del contribuente, soprattutto se effettuata sulla base delle numerose tipologie di dati posseduti e attraverso l'attribuzione di un profilo, presenta rischi specifici per i diritti fondamentali e la libertà, nonché la dignità degli interessati, che richiedono la previsione di adeguate garanzie. Ciò, in particolare, laddove vengano utilizzate tecniche che rendono possibile collocare gli individui in classi al fine di prendere decisioni sul loro conto (artt. 14 e 17 del Codice).

Il Garante ha esaminato la correttezza e la liceità del trattamento posto in essere dall'Agenzia delle entrate al fine di individuare, in applicazione del Codice, le garanzie da assicurare in relazione alla natura e alla qualità dei dati, alle modalità del trattamento e agli effetti che lo stesso può determinare sugli interessati, introducendo, in particolare, misure e accorgimenti idonei a correggere fattori che generino imprecisioni nei dati, assicurandone l'esattezza e limitando i rischi di errori inerenti alla profilazione, considerato che eventuali imprecisioni nella fase di raccolta di informazioni sono destinate a ripercuotersi, con esiti imprevedibili, sulle determinazioni assunte sulla base di un loro trattamento automatizzato, anche con rilevanti conseguenze in capo agli interessati. Particolare attenzione è stata prestata all'informativa e all'esercizio dei diritti da parte degli interessati, anche nel corso del procedimento amministrativo tributario condotto dall'Agenzia.

La verifica preliminare è stata compiuta anche attraverso accertamenti mirati di carattere ispettivo volti a verificare in concreto il trattamento dei dati contenuti nell'Anagrafe tributaria anche attraverso l'applicativo appositamente realizzato. Nell'ambito di tale procedimento numerose sono state le occasioni di proficuo confronto con l'Agenzia al fine di meglio comprendere le criticità riscontrate e di individuare congiuntamente soluzioni volte a contemperare le esigenze della lotta all'evasione fiscale con il rispetto del diritto alla protezione dei dati personali degli interessati nonché dei principi previsti dal Codice (primo fra tutti quello della qualità dei dati).

Nell'ambito dell'istruttoria sono emersi numerosi profili di criticità che rendevano il sistema non conforme al Codice, derivanti principalmente dal fatto che lo stesso decreto ministeriale di attuazione del nuovo redditometro non era stato sottoposto al previsto parere del Garante, il quale avrebbe così potuto notevolmente anticipare e contribuire a risolvere talune problematiche che, invece, sono emerse solo nel corso della verifica preliminare. Più precisamente, tali criticità hanno riguardato la qualità e l'esattezza dei dati utilizzati dall'Agenzia delle entrate, l'individuazione in via presuntiva della spesa sostenuta da ciascun contribuente riguardo ad ogni aspetto della vita quotidiana (tempo libero, libri, pasti fuori casa, *etc.*) mediante l'attribuzione alla gene-

ralità dei soggetti censiti nell'Anagrafe tributaria della spesa media rilevata dall'Istat, alle informazioni oggetto di esame in contraddittorio con l'Agenzia e all'informativa da rendere al contribuente, con particolare riguardo alle conseguenze sul mancato conferimento dei dati in tutte le fasi del procedimento amministrativo.

Alcune di queste criticità sono state risolte già nel corso della verifica preliminare mediante i correttivi apportati dall'Agenzia delle entrate, anche su indicazione dell'Ufficio. Ulteriori misure a garanzia dei contribuenti sono state quindi prescritte dall'Autorità con il provvedimento del 21 novembre 2013, n. 515 (doc. web n. 2765110).

In particolare, il Garante ha ritenuto che il decreto ministeriale, nella parte in cui prevede la profilazione del contribuente attraverso l'imputazione presuntiva di elementi di capacità contributiva relativi ad ogni singolo aspetto della vita quotidiana – il cui contenuto induttivo è determinato mediante l'utilizzo di spese medie (e, in particolare, di quelle rilevate a fini statistici dall'Istat), non finalizzate alla valorizzazione di un elemento di capacità contributiva certo, e quindi non ancorate all'esistenza di un bene o un servizio e al relativo mantenimento – costituisca un'ingerenza ingiustificata nella vita privata degli interessati in quanto sproporzionata rispetto alle legittime finalità di interesse generale perseguite dall'Agenzia. Ciò va oltre quanto necessario per ricostruire sinteticamente il reddito del contribuente ai sensi dell'art. 38, d.P.R. n. 600/1973 e si pone in contrasto con i principi di correttezza e liceità del trattamento nonché di esattezza dei dati, specie per i profili relativi all'attribuzione delle spese Istat (artt. 2 e 11 del Codice).

Ugualmente, ad avviso del Garante, la circostanza di dover discutere dell'ammontare delle voci di spesa riguardanti ogni singolo aspetto della vita quotidiana con l'amministrazione finanziaria – come proposto dall'Agenzia quale correttivo per circoscrivere l'inesattezza del trattamento derivante dall'utilizzo presuntivo delle spese medie Istat – espone il contribuente a una forte invasione della propria sfera privata, trovandosi lo stesso obbligato a dover giustificare di aver o, soprattutto, non aver sostenuto certe tipologie di spesa, anche relative alle sfere più intime della personalità (cfr. ad es., tempo libero, istruzione dei figli, *etc.*) e a portare a conoscenza nel dettaglio il funzionario dell'Agenzia del proprio stile di vita. Pertanto, a fronte delle criticità evidenziate nell'istruttoria, l'Autorità ha rilevato che anche la raccolta in contraddittorio da parte dell'Agenzia di informazioni relative ad ogni singolo aspetto della vita quotidiana a fini di controllo fiscale, anche risalente nel tempo, seppur effettuato per una rilevante finalità di interesse pubblico, entra in conflitto con i principi in materia di riservatezza e protezione dei dati personali e, in particolare, con l'art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali il quale, come noto, prevede che, in una società democratica, l'ingerenza di una autorità pubblica nella vita privata e familiare dell'individuo, ancorché prevista dalla legge, debba essere necessaria e proporzionata.

Alla luce di queste considerazioni, possono così riassumersi le misure che il Garante ha prescritto all'Agenzia delle entrate per rendere il nuovo redditometro conforme al Codice:

- (Profilazione) il reddito del contribuente può essere ricostruito utilizzando unicamente spese certe e spese che valorizzano elementi certi (possesso di beni o utilizzo di servizi e relativo mantenimento) senza utilizzare spese presunte basate unicamente sulla media Istat;
- (Spese medie Istat) i dati delle spese medie Istat non possono essere utilizzati per determinare l'ammontare di spese frazionate e ricorrenti (es., abbigliamento, alimentari, alberghi, *etc.*) per le quali il fisco non ha evidenze certe. Anche sulla base di elementi forniti dall'Istat, è emerso che tali dati, riferibili

allo *standard* di consumo medio familiare, non possono essere ricondotti correttamente ad alcun individuo, se non con notevoli margini di errore, in eccesso o in difetto;

- (Fitto figurativo) il cd. fitto figurativo (attribuito al contribuente in assenza di abitazione in proprietà o locazione nel comune di residenza) non deve essere utilizzato per selezionare i contribuenti da sottoporre ad accertamento, ma solo ove necessario a seguito del contraddittorio. Il fitto figurativo dovrà essere attribuito solo una volta verificata la corretta composizione del nucleo familiare presso l'anagrafe, per evitare le notevoli incongruenze riscontrate dal Garante (che comportavano, ad es., l'attribuzione automatica a 2 milioni di minori della spesa fittizia per l'affitto di una abitazione);
- (Esattezza dei dati) l'Agenzia deve porre particolare attenzione alla qualità e all'esattezza dei dati al fine di prevenire e correggere le evidenti anomalie riscontrate nella banca dati o i disallineamenti tra famiglia fiscale e anagrafica. La corretta composizione della famiglia è infatti rilevante per la ricostruzione del reddito familiare, l'individuazione della tipologia di famiglia o l'attribuzione del cd. fitto figurativo;
- (Informativa ai contribuenti) il contribuente deve essere informato, attraverso l'apposita informativa allegata al modello di dichiarazione dei redditi e disponibile anche sul sito dell'Agenzia delle entrate, del fatto che i suoi dati personali saranno utilizzati anche ai fini del reddirometro. Nell'invito al contraddittorio devono essere specificati chiaramente al contribuente i poteri utilizzati dall'Agenzia delle entrate nell'ambito del trattamento dei suoi dati personali effettuato ai fini di accertamento sintetico ai sensi del citato art. 38, chiarendo la natura obbligatoria o facoltativa degli ulteriori dati richiesti dall'Agenzia (es. dati finanziari) e le conseguenze di un eventuale rifiuto anche parziale a rispondere;
- (Contraddittorio) dati presunti di spesa, non ancorati ad alcun elemento certo e quantificabili esclusivamente sulla base delle spese Istat relativi ad ogni aspetto della vita quotidiana, anche risalenti nel tempo, non possono costituire oggetto del contraddittorio.

Comunicazioni all'Anagrafe tributaria

Il Garante ha esaminato lo schema di provvedimento del direttore dell'Agenzia delle entrate in materia di comunicazioni all'Anagrafe tributaria dei dati relativi ai contratti e ai premi assicurativi e volto a riunire in un unico tracciato *record* comunicazioni relative ai premi assicurativi versati e ai dati dei contratti di assicurazione, semplificando le trasmissioni effettuate dalle compagnie di assicurazione e da altri soggetti del settore ed evitando ogni rischio di duplicazione dei dati.

Nel corso dell'istruttoria l'Autorità ha approfondito la questione anche attraverso un accertamento di carattere ispettivo presso l'Agenzia delle entrate al fine di acquisire ogni informazione utile a valutare la pertinenza e la non eccedenza delle informazioni raccolte relative alla voce "contributo al Servizio sanitario nazionale" del tracciato *record* che le compagnie di assicurazione e altri soggetti del settore avrebbero dovuto trasmettere all'Anagrafe tributaria, rispetto alle finalità di controllo formale degli oneri deducibili perseguite dalla norma, anche tenuto conto dei dati relativi alle assicurazioni e ai beni mobili registrati già presenti in Anagrafe tributaria, o comunque disponibili all'Agenzia delle entrate. In particolare, è stata verificata la pertinenza rispetto:

- alla richiesta dei dati relativi all'importo del premio, alla targa del mezzo e alla potenza del motore (Kw/CV) a fronte delle informazioni già rilevabili dal pubblico registro automobilistico, nonché da altre comunicazioni all'Anagrafe tributaria;

- ai dati raccolti sulla base del provvedimento del direttore dell'Agenzia delle entrate del 20 aprile 2012 che prevede la trasmissione telematica della comunicazione degli importi annualmente versati alle province relativi ai contratti di assicurazione contro la responsabilità civile;
- alla soglia prevista per la deducibilità di tale contributo alla luce delle recenti modifiche normative introdotte dall'art. 4, comma 76, l. n. 92/2012, che ne hanno limitato la rilevanza ai soli casi in cui l'importo sia superiore a euro 40.

In relazione agli autoveicoli è risultato quindi possibile limitare la comunicazione – rispetto a quanto inizialmente previsto – ai campi strettamente necessari relativi all'identificativo del contratto di polizza, alla data di stipula del contratto, all'oggetto del contratto e alla targa del veicolo, in quanto i dati relativi alla potenza del motore e all'ammontare totale del premio possono essere acquisiti, rispettivamente, dal pubblico registro automobilistico e dai dati comunicati all'Anagrafe tributaria dalle assicurazioni ai sensi del provvedimento del Direttore dell'Agenzia del 20 aprile 2012, relativo ai soli veicoli a motore.

Con riferimento alla soglia prevista per la deducibilità del contributo al Ssn, introdotta dall'art. 4, comma 76, l. n. 92/2012, l'Agenzia ha ritenuto altresì di poter limitare l'obbligo di comunicazione ai casi in cui l'importo sia superiore a euro 40, modificando il tracciato record affinché risulti chiaro che, nel caso in cui il contributo sia inferiore a detta soglia, gli elementi dell'intero tracciato non devono essere compilati.

Riguardo alle modalità tecniche di scambio dei dati, considerato che lo schema ha previsto che i soggetti obbligati effettuino le comunicazioni previste utilizzando il servizio telematico Entrarel o Fisconline, già oggetto di rilievi critici del Garante con il provvedimento del 17 aprile 2012, n. 145 (doc. web n. 1886775), l'Agenzia ha dichiarato che tali comunicazioni saranno trasferite sulla nuova infrastruttura Sistema di interscambio dati (Sid) in corso di realizzazione, già valutato favorevolmente del Garante nel parere del 15 novembre 2012, n. 861 (doc. web n. 2099774) e nel provvedimento del 31 gennaio 2013, n. 48 (doc. web n. 2268436), e che, comunque, sono stati pianificati alcuni interventi evolutivi del servizio telematico Entratel riferiti, in particolare, alla gestione della dimensione dei *file* e al monitoraggio dell'utilizzo delle credenziali di accesso.

Il Garante, pertanto, a seguito delle modifiche apportate, ha espresso parere favorevole sulla successiva versione dello schema di provvedimento predisposta dell'Agenzia, che ha tenuto conto degli approfondimenti richiesti dall'Ufficio relativi alla pertinenza e non eccedenza dei dati, a condizione che tali comunicazioni fossero trasferite sulla nuova infrastruttura Sid entro il 31 dicembre 2013 (provv. 4 aprile 2013, n. 153, doc. web n. 2462488).

Accesso all'Archivio dei rapporti finanziari

L'Agenzia delle entrate ha chiesto al Garante chiarimenti in ordine ad una sentenza del Tar Lazio del 21 ottobre 2013, n. 9036, secondo cui, tra i "documenti fiscali" che l'Agenzia delle entrate dovrebbe esibire ad un ricorrente ai sensi della l. n. 241/1990, rientrerebbero anche le "comunicazioni inviate da tutti gli operatori finanziari dell'Anagrafe tributaria – sezione Archivio dei rapporti finanziari – relative ai rapporti continuativi, alle operazioni di natura finanziaria ed ai rapporti di qualsiasi genere".

In relazione a quanto rappresentato dall'Agenzia, l'Autorità ha deciso di dare mandato all'Avvocatura dello Stato per impugnare la sentenza e ha evidenziato in un'apposita nota alla stessa Agenzia, oltre a più generali criticità in ordine all'applicabilità del concetto stesso di documento amministrativo a tal genere di banca dati, che una simile applicazione della disciplina sull'accesso ai documenti amministrativi si pone in contrasto con i diritti e le libertà fondamentali nonché con la dignità

degli interessati, beni tutelati dalla normativa, anche di rilevanza comunitaria, in materia di protezione dei dati personali, specie con riferimento all'eccezionale concentrazione presso l'Archivio dei rapporti finanziari (che costituisce un'apposita sezione separata dell'Anagrafe tributaria) di un'enorme quantità di informazioni personali riferibili alla totalità dei contribuenti, con ciò snaturando le specifiche ed emergenziali finalità di contrasto all'evasione fiscale che hanno legittimato la costituzione di tale banca dati.

Dalla documentazione disponibile al Garante, risulta infatti che l'Archivio dei rapporti finanziari contenga circa 600.000.000 (seicento milioni) di rapporti attivi e che annualmente gli operatori finanziari effettuano circa 155.000.000 (centocinquantacinque milioni) di comunicazioni relative alle sole variazioni dei rapporti in essere e alle cd. operazioni extraconto.

La legge stabilisce tassativamente i soggetti e le specifiche finalità per cui tali dati possono essere utilizzati. Ad esempio, oltre all'autorità giudiziaria e per specifiche finalità antimafia e antiterrorismo, l'Agenzia può farvi accesso unicamente a seguito dell'avvio di indagini finanziarie per le attività connesse all'accertamento sulle imposte dei redditi e sul valore aggiunto ed alla riscossione mediante ruolo, nonché, con riferimento ai cd. dati contabili raccolti a partire dal 2011, unicamente con modalità centralizzate per la formazione di liste selettive di contribuenti a maggior rischio evasione.

Estendere l'utilizzo delle informazioni contenute nelle comunicazioni degli operatori finanziari all'Archivio dei rapporti in assenza dei (e, quindi oltre, i) predetti presupposti soggettivi e oggettivi tassativamente individuati dal legislatore come prefigurato dalla citata sentenza del Tar del Lazio significherebbe, di fatto, equiparare il penetrante potere d'indagine dell'Agenzia delle entrate e quello riservato all'accertamento di fattispecie penalmente rilevanti a quello di chiunque risultasse portatore di un interesse e quindi anche di altri innumerevoli soggetti (pubbliche amministrazioni e imprese). Con ciò superando i limiti imposti dal legislatore nella costituzione di tale Archivio ed esponendo la totalità dei contribuenti ad una sproporzionata invasione della propria vita privata, in conflitto con la necessità di rispettare i limiti posti dai principi in materia di riservatezza e protezione dei dati personali e, in particolare, dall'art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (nota 20 dicembre 2013).

4.8. *La videosorveglianza in ambito pubblico*

Anche nel corso del 2013, frequenti richieste si sono incentrate sulla necessità di sottoporre (o meno) alla verifica preliminare dell'Autorità sistemi di videosorveglianza (come previsto nel provvedimento generale in materia di videosorveglianza dell'8 aprile 2010, doc. web n. 1712680).

Riconoscimento facciale e veicolare

A tal riguardo, in presenza di una richiesta di autorizzazione e di verifica preliminare ai sensi dell'art. 17 del Codice da parte di un comune in relazione al trattamento di dati personali che intendeva effettuare tramite sistemi di videosorveglianza intelligenti "con riconoscimento facciale e veicolare dei trasgressori", per controllare il deposito di rifiuti domestici in orari non consentiti nonché di rifiuti ingombranti, inquinanti e pericolosi, al fine di procedere alla relativa contestazione dei verbali di violazione, l'Ufficio ha fornito alcuni chiarimenti in ordine all'autorizzazione e ha manifestato l'esigenza di conoscere taluni elementi utili alla istruttoria (tra i quali la modalità di funzionamento del sistema di riconoscimento delle caratteristiche fisionomiche degli interessati, l'eventuale collegamento, incrocio o confronto con altri dati perso-

nali, il contesto in cui il predetto sistema sarebbe stato installato nonché l'eventuale capacità dello stesso di rilevare i percorsi degli interessati). Poiché gli elementi forniti dal comune non risultavano rientrare tra le ipotesi individuate nel provvedimento generale del 2010 in cui è necessario sottoporre i sistemi di videosorveglianza alla verifica preliminare dell'Autorità, non è stato dato seguito alla richiesta (note 13 settembre 2013 e 8 gennaio 2014).

Un'azienda di trasporti, *partner* di un progetto europeo volto a sviluppare un sistema di sicurezza del trasporto pubblico nelle città europee, ha chiesto la verifica preliminare per i trattamenti di dati personali effettuati tramite sistemi di videosorveglianza "intelligenti" ideati per la realizzazione del progetto. A seguito di un incontro svoltosi presso l'Ufficio, è stato precisato che, in realtà, si sarebbero realizzate soltanto delle rappresentazioni con attori consenzienti e che l'azienda non avrebbe, quindi, trattato alcun dato personale dei passeggeri del trasporto pubblico. Nel prendere atto di quanto dichiarato, l'Ufficio ha comunicato l'archiviazione della richiesta (nota 26 giugno 2013).

Monitoraggio del traffico acqueo

Anche la Città di Venezia ha formulato una richiesta di verifica preliminare in ordine ad un sistema di videosorveglianza denominato "Argos" volto a monitorare la navigazione nei rii, canali e tratti più interessati dal traffico acqueo. Al fine di acquisire elementi necessari all'esame dei sistemi da utilizzare, sono stati avviati contatti per le vie brevi e richiesti chiarimenti, anche in vista di un incontro da tenersi presso la sede dell'Ufficio. Alla luce delle indicazioni fornite, il trattamento dei dati personali non è risultato da qualificare tra quelli da sottoporre alla verifica preliminare dell'Autorità.

Grande Progetto Pompei

È stato dato seguito, invece, ad una richiesta di verifica preliminare presentata dalla Soprintendenza Speciale per i beni archeologici di Napoli e Pompei in relazione all'intenzione di allungare i tempi di conservazione delle immagini raccolte tramite il "Sistema di videosorveglianza dell'area archeologica di Pompei". La Soprintendenza ha sottoposto al Garante la richiesta di prolungamento del periodo di conservazione delle immagini registrate mediante talune telecamere dedicate a sorvegliare i cantieri e le aree di stoccaggio del "Grande Progetto Pompei" nonché i varchi di accesso riservati al transito del personale e dei mezzi diretti ai cantieri medesimi, per un periodo superiore alla settimana, presentando, a supporto di tale istanza, una richiesta della Direzione investigativa antimafia - Centro operativo di Napoli. Al riguardo, la citata Direzione aveva valutato che l'arco temporale individuato appariva adeguato in considerazione dei tempi occorrenti per il restauro dei diversi siti archeologici, considerato che le relative fasi di fornitura dei materiali o il noleggio di mezzi, normalmente si esauriscono all'interno di tale periodo temporale.

La Soprintendenza Speciale ha dichiarato che l'attività di videosorveglianza interessata dalla verifica preliminare avrebbe supportato l'attività della Prefettura volta a controllare, soprattutto a fini di prevenzione antimafia, la regolarità degli accessi e delle presenze in cantiere e non sarebbe stata quindi finalizzata al controllo dell'attività dei lavoratori.

L'Autorità ha richiamato il provvedimento generale dell'8 aprile 2010 e le speciali disposizioni di legge, entrate in vigore prima della normativa in materia di protezione dei dati personali, che prevedono la possibilità di installare impianti audiovisivi presso i musei statali per il controllo continuativo ed ininterrotto dei beni culturali esposti o depositati, con finalità di prevenzione e di tutela da azioni criminose e danneggiamenti (d.l. 14 novembre 1992, n. 433, convertito, con modificazioni, dalla l. 14 gennaio 1993, n. 4); considerati quindi gli elementi acquisiti, anche sulla scorta delle valutazioni espresse dalla Direzione investigativa antimafia, è stata ritenuta sussistente una specifica esigenza di sicurezza, in relazione ad una concreta

situazione di rischio. È stato pertanto ritenuto congruo un allungamento dei tempi di conservazione delle immagini per il periodo richiesto, in quanto rispettoso del principio di proporzionalità, che prevede la conservazione dei dati personali oggetto di trattamento, in una forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati (art. 11, comma 1, lett. *e*), del Codice; punto 3.4. del citato provvedimento), pendente la rappresentata eccezionale necessità. È stato comunque precisato che, ove l'attività di sorveglianza dei cantieri consenta, pur non essendovi preordinata, un controllo a distanza dell'attività dei lavoratori, resta ferma l'esigenza che venga rispettato il provvedimento generale del Garante dell'8 aprile 2010, con particolare riferimento alle garanzie previste per i lavoratori dagli artt. 114 del Codice e 4, l. 20 maggio 1970, n. 300 (provv. 3 ottobre 2013, n. 428, doc. web n. 2724840).

Tempi di conservazione delle immagini

Analogamente, con riferimento all'istanza presentata da Sogei per ottenere l'autorizzazione all'allungamento dei tempi di conservazione delle immagini videoregistrate presso la sede della società, il Garante ha ammesso la conservazione per trenta giorni delle immagini raccolte attraverso il sistema di videosorveglianza. È stata valutata, infatti, la peculiarità dell'attività di Sogei, che conserva e custodisce nella propria banca dati l'intera Anagrafe tributaria, il cui Sistema Informativo della Fiscalità è fra i più complessi e strategici nell'ambito della p.a.

Il sistema di videosorveglianza descritto ha la finalità di proteggere le banche dati da accessi non autorizzati e di tutelare le apparecchiature *hardware* e i prodotti *software* utilizzati per la loro gestione, nonché i beni e le persone che operano all'interno dei locali e nelle aree aziendali. La richiesta di estendere il periodo di conservazione delle immagini era stata motivata, in particolare, da specifiche esigenze di sicurezza finalizzate a prevenire minacce terroristiche, rischi di intrusione e possibili azioni criminose e in alcun modo finalizzata ad un controllo dell'attività dei lavoratori.

Nell'accogliere la richiesta presentata, il Garante ha tenuto conto della particolare delicatezza e della mole dei dati trattati dall'Anagrafe tributaria nonché delle specifiche esigenze di sicurezza e di protezione di banche dati, beni aziendali e persone, in relazione ad una concreta situazione di rischio, valutata anche dal Ministero dell'economia e delle finanze - Organo centrale di sicurezza (provv. 28 novembre 2013, n. 532, doc. web n. 2803442).

Anche l'Enea (Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile) - Centro ricerche Frascati, ha richiesto al Garante di poter allungare i tempi di conservazione delle immagini raccolte mediante i sistemi di videosorveglianza fino a quarrordici giorni durante i periodi di chiusura del Centro. Tale richiesta è stata motivata sulla base della necessità di impedire l'accesso fraudolento in alcuni locali dove si trovano impianti e/o sostanze potenzialmente nocive per la salute, nonché ulteriori furti di rame, considerato il frequente susseguirsi di tali eventi, da considerarsi "altamente probabili e quindi incombenti".

A sostegno della citata richiesta, l'Agenzia ha rappresentato che nei laboratori del Centro vengono effettuate attività di ricerca e sviluppo di applicazioni delle radiazioni relative a sorgenti laser (a gas, a sraro solido, a elettroni liberi) e applicazioni laser nel campo della diagnostica (ambientale, industriale e medicale) dei nano e micro sistemi, della metrologia e della visione laser; da ciò deriverebbero specifici rischi legati all'utilizzo di sostanze chimiche, gas pericolosi e radiazioni non ionizzanti e, con particolare riguardo alle attività nucleari, anche rischi di eventi delittuosi gravi.

Infine, è stato assicurato che, decorso il periodo di conservazione, le registrazioni verrebbero cancellate e comunque non utilizzate per il controllo a distanza dei dipendenti.

La specifica esigenza di sicurezza, riconnessa alla delicatezza dell'attività di ricerca svolta e ai concreti rischi di sottrazione indebita di materiali ed apparecchiature ha indotto il Garante ad accogliere la richiesta di verifica preliminare relativa all'allungamento dei tempi di conservazione delle immagini registrate dagli impianti di videosorveglianza dall'Enea, chiarendo che l'accesso alle stesse avrebbe potuto essere effettuato solo nel caso in cui fossero ravvisati o segnalati eventuali illeciti oppure in caso di richiesta in tal senso da parte dell'autorità giudiziaria (provv. 11 aprile 2013, n. 178, doc. web n. 2464185).

Sistemi di videosorveglianza "intelligenti"

Le richieste di verifica preliminare non hanno riguardato soltanto l'allungamento dei tempi di conservazione delle immagini, ma anche trattamenti di dati personali effettuati tramite sistemi di videosorveglianza cd. "intelligenti". Si fa riferimento, segnatamente, alla richiesta di attivazione da parte di un comune di un particolare sistema di videosorveglianza nell'ambito dell'attività di sicurezza urbana, al fine di evitare atti vandalici e danneggiamenti a monumenti e sedi istituzionali. In particolare, il sistema di videosorveglianza sottoposto all'esame dell'Autorità risultava composto da dieci telecamere, con inquadratura fissa, che avrebbero azionato un allarme, a seguito della rilevazione della permanenza prolungata da parte di un individuo, per oltre 30 secondi, nell'area virtuale contrassegnata da un'immaginaria linea di interdizione adiacente ai siti monumentali, e per oltre 60 secondi, per quella situata in prossimità delle sedi istituzionali. L'allarme, di tipo ottico/acustico, si sarebbe manifestato sul monitor della postazione di controllo, richiamando l'attenzione dell'operatore di polizia locale addetto alla centrale operativa per il quale si sarebbero rese visibili le informazioni dettagliate dell'evento, al fine di consentire un eventuale pronto intervento.

Il sistema descritto, in base al provvedimento del 2010 in materia di videosorveglianza, era stato correttamente sottoposto alla verifica preliminare dell'Autorità, in quanto rientrante tra i sistemi di ripresa "intelligenti" che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli ed eventualmente registrarli. Il Garante si è quindi espresso evidenziando che il sistema, per le sue caratteristiche, non avrebbe comportato in concreto un pregiudizio rilevante per i diritti e le libertà fondamentali dei cittadini, in quanto, nel rilevare la presenza prolungata degli interessati nell'area adiacente ai monumenti e alle sedi istituzionali, avrebbe avuto come unico effetto quello di richiamare l'attenzione dell'operatore di polizia addetto alla centrale operativa al fine di favorire, se necessario, un tempestivo intervento. Dalla documentazione trasmessa in atti non è risultata l'attivazione di ulteriori funzionalità del sistema, eventualmente legate al comportamento dell'interessato ripreso, quali, ad esempio, la capacità di rilevarne i percorsi, l'analisi audio, la geolocalizzazione o il riconoscimento tramite incrocio con ulteriori specifici dati personali o confronto con una campionatura precostituita.

Il Garante ha ritenuto quindi proporzionato il trattamento dei dati personali che il comune intendeva effettuare per le finalità di sicurezza urbana, valutata l'esigenza di tutela dei siti monumentali – già oggetto di atti vandalici – e istituzionali, nonché la dichiarata inadeguatezza delle misure di controllo alternative determinata dall'esiguità del personale a disposizione. L'Autorità ha però richiesto che nell'informativa fossero chiaramente evidenziate le caratteristiche del sistema (con particolare riguardo alla rilevazione e segnalazione della presenza prolungata nelle aree delimitate dalla linea di interdizione virtuale in prossimità delle sedi e degli edifici selezionati), richiamando altresì l'attenzione sulle misure di sicurezza da adottare, al fine di consentire, in particolare, la verifica delle attività sugli accessi alle immagini o sul controllo dei sistemi di ripresa, nonché sulla necessità di rispettare i tempi limitati di conservazione delle immagini registrate (provv. 21 marzo 2013, n. 136, doc. web n. 2380059).

Sistemi mobili di videosorveglianza

Sono stati altresì forniti chiarimenti in merito all'installazione di sistemi di videosorveglianza mobili, a seguito di una specifica istanza formulata da un comune che intendeva installare tali sistemi "al fine di combattere efficacemente il dilagante fenomeno dell'abbandono incontrollato di rifiuti (pericolosi e non) nel centro abitato e nelle campagne". Al riguardo è stato rappresentato che l'utilizzo di sistemi di videosorveglianza, anche di tipo mobile, risulta lecito con riferimento alle attività di controllo volte ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli inefficace, il ricorso a strumenti e sistemi di controllo alternativi (cfr. punto 5.2. del provvedimento generale). Analogamente, l'utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (nota 19 novembre 2013).

Sempre con riferimento a sistemi mobili di videosorveglianza, si menziona la richiesta di chiarimenti da parte del Dipartimento vigili del fuoco-soccorso pubblico e difesa civile in ordine alla possibilità di equipaggiare i veicoli in dotazione, impegnati nel servizio di soccorso tecnico urgente, di un sistema di apparati mobili di videosorveglianza di bordo; ciò consentirebbe la registrazione di flussi audio-video georeferenziali e la trasmissione in tempo reale delle informazioni rilevate alla sala operativa di ciascun Comando provinciale, competente per territorio, e al sistema centrale di gestione ubicato presso il Comando provinciale di Napoli.

Al riguardo, l'Ufficio ha rilevato che talune disposizioni del Codice, tra le quali quella riguardante l'obbligo di fornire una preventiva informativa agli interessati, non sono applicabili al trattamento di dati personali effettuato, anche sotto forma di suoni e immagini, dal Centro elaborazione dati del Dipartimento di pubblica sicurezza o da Forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, ove effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento (art. 53 del Codice).

Alla luce di tale previsione, è stato rappresentato che per i predetti titolari del trattamento, tra i quali rientrano anche gli appartenenti al Corpo dei vigili del fuoco (art. 8, l. 27 dicembre 1941, n. 1570) quando pongono in essere trattamenti riconducibili a quelli previsti dall'art. 53 del Codice – relativi, ad esempio, al contrasto di atti criminosi compiuti con l'uso di armi nucleari, batteriologiche, chimiche e radiologiche (cfr. art. 24, comma 5, lett. *a*), d.lgs. 8 marzo 2006, n. 139) –, vale la regola secondo la quale l'informativa può non essere resa, sempre che appunto i dati personali siano trattati per il perseguimento delle finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati e il trattamento sia comunque effettuato in base ad espressa disposizione di legge che lo preveda specificamente.

Al fine di rafforzare la tutela dei diritti e delle libertà fondamentali degli interessati, l'Autorità ha tuttavia ritenuto fortemente auspicabile che l'informativa – benché non obbligatoria, laddove l'attività di videosorveglianza sia espletata ai sensi dell'art. 53 del Codice – sia comunque resa in tutti i casi nei quali non ostano in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati. Ciò naturalmente all'esito di un prudente apprezzamento volto a verificare che l'informativa non ostacoli, ma anzi rafforzi, in concreto l'espletamento delle specifiche funzioni perseguite, tenuto anche conto che rendere palese l'utilizzo dei sistemi di videosorveglianza può, in molti casi, svolgere una efficace

funzione di deterrenza; in ogni caso, anche se i titolari si avvalessero della facoltà di fornire l'informativa, resta salva la non applicazione delle restanti disposizioni del Codice tassativamente indicate dall'art. 53, comma 1, lett. *a*) e *b*).

È stato sottolineato, al contrario, che deve essere fornita un'idonea informativa in tutti i casi in cui i trattamenti di dati personali effettuati tramite l'utilizzo di sistemi di videosorveglianza dalle Forze di polizia, dagli organi di pubblica sicurezza e da altri soggetti pubblici non siano riconducibili a quelli espressamente previsti dall'art. 53 del Codice (cfr. punti 3.1.1. e 3.1.2. del provvedimento generale del 2010) (nota 5 marzo 2013).

Videosorveglianza di area marina protetta

L'Autorità è altresì intervenuta, a seguito di notizie riportate dagli organi di informazione, per verificare la correttezza del trattamento dei dati personali effettuato tramite un sistema di videosorveglianza previsto presso il territorio costiero dell'area marina protetta Penisola del Sinis-Isola di Mal di Ventre da un comune sardo in collaborazione con l'Agenzia conservatoria delle coste della Sardegna; in particolare, sono stati richiesti elementi in ordine alle modalità di configurazione del sistema con le quali si sarebbe inteso garantire il rispetto dei principi di necessità e di proporzionalità sia nella scelta della modalità di ripresa e di dislocazione delle telecamere, sia nelle varie fasi del trattamento, avendo cura di specificare l'eventuale identificabilità dei soggetti ripresi nonché se fosse previsto l'inserimento delle immagini raccolte sulla rete internet (nota 17 giugno 2013). Al riguardo, il comune ha chiarito che le telecamere, ancora da attivare e preordinate a verificare le condizioni meteo-marine nonché a valutare l'erosione costiera, sarebbero state configurate in modo da non consentire di effettuare riprese particolareggiate tali da rendere identificabili i soggetti ripresi.

Sempre in tema di videosorveglianza di aree marine, un comune sardo ha comunicato all'Autorità l'intenzione di installare alcune *webcam* presso spiagge e punti panoramici, con finalità di promozione turistica. Al riguardo, è stato evidenziato che l'attività di rilevazione di immagini a scopi promozionali-turistici deve avvenire con modalità che rendano non identificabili i soggetti ripresi. Ciò in considerazione delle peculiari modalità del trattamento, dalle quali deriva un concreto rischio del verificarsi di un pregiudizio rilevante per gli interessati: le immagini raccolte tramite tali sistemi, infatti, vengono inserite direttamente sulla rete internet, consentendo a chiunque navighi sul web di visualizzare in tempo reale i soggetti ripresi e di utilizzare le medesime immagini anche per scopi diversi dalle finalità promozionali-turistiche o pubblicitarie perseguite dal titolare del trattamento (punto 4.5 del provvedimento generale del 2010) (nota 22 luglio 2013).

Limiti di velocità

L'Ufficio è stato interpellato dal Dipartimento per i trasporti, la navigazione e i sistemi informativi e statistici del Ministero delle infrastrutture e dei trasporti in ordine alla legittimità di un dispositivo per l'accertamento a distanza della violazione del limite di velocità – rispetto al quale aveva ricevuto una richiesta di omologazione – anche attraverso riprese frontali del veicolo con il quale viene commessa l'infrazione. Sul punto, come evidenziato nel corso di un incontro preliminare, sono state richiamate le indicazioni fornite dal Garante nel provvedimento del 2010, precisando che, in conformità al quadro normativo di settore in materia di violazioni al codice della strada, le risultanze video/fotografiche devono contenere solo gli elementi previsti per la predisposizione del verbale di accertamento delle violazioni (tra i quali, il giorno, l'ora e la località nei quali la violazione è avvenuta, le generalità e residenza del trasgressore, la targa di riconoscimento, la sommaria esposizione del fatto, nonché la citazione della norma violata, cfr. art. 383, d.P.R. n. 495/1992); pertanto, devono essere oscurate le immagini rilevate incidentalmente, non pertinenti rispetto alla finalità di predisposizione del verbale di accertamento delle violazioni (nota 25 luglio 2013).

Da ultimo, il Garante è intervenuto in merito alla possibilità che gli organismi sanitari possano usare sistemi di videosorveglianza all'interno dei propri servizi igienici per il controllo della procedura di raccolta del campione urinario per accertare l'assenza di tossicodipendenza a fini certificatori, nonché di cura della salute, individuando talune cautele ed accorgimenti in un provvedimento generale (provv. 15 maggio 2013, n. 243, doc. web n. 2475383), più diffusamente descritto nel par. 5.1.

4.9: *I trattamenti effettuati presso regioni ed enti locali*

La disciplina in materia di protezione dei dati personali continua a presentare criticità in ambito locale e regionale.

L'Ufficio è intervenuto con riferimento al quesito sottoposto da un comune in ordine all'utilizzo di apparecchiature video durante la seduta del consiglio comunale. A tal proposito, è stato rappresentato che il testo unico delle leggi sull'ordinamento degli enti locali stabilisce espressamente che gli atti e le sedute del consiglio comunale e delle commissioni sono pubbliche, salvi i casi previsti dal regolamento. Pertanto, si è ritenuto che spetti all'amministrazione comunale introdurre eventuali limiti a detto regime di pubblicità mediante un atto di natura regolamentare (artt. 10 e 38, d.lgs. 18 agosto 2000, n. 267) e che non competa all'Autorità sindacare le scelte effettuate con il regolamento nel quale si sono disciplinati i limiti e le modalità di pubblicità delle sedute consiliari. Ove sia consentita l'effettuazione di riprese delle sedute del consiglio comunale, agli interessati deve essere fornita, da parte del comune, l'informativa prevista dall'art. 13 del Codice (nota 1° ottobre 2013).

Outsourcing nella p.a.

Si segnala il riproporsi della problematica inerente al trattamento dei dati effettuato da soggetti esterni all'amministrazione comunale per l'esercizio di funzioni istituzionali (*outsourcing*). In particolare, un'associazione di consumatori ha formulato un quesito in ordine alla possibilità per la polizia municipale di affidare al personale di società il trattamento di dati personali effettuato, dopo l'accertamento da parte degli agenti della polizia municipale, di attività quali la digitalizzazione delle immagini derivanti da fotogrammi acquisite da apparecchiature *autovelox*, la stampa delle visure del Pubblico registro automobilistico (Pra), la stampa di verbali, *etc.*

Analogamente sono pervenute segnalazione di cittadini relative alla notifica di verbali di infrazione delle disposizioni del codice della strada a mezzo di società cui vengono affidate dai comuni le attività di stampa, imbustamento e spedizione dei verbali.

In proposito è stato rappresentato che nello svolgimento dei propri compiti istituzionali, ciascun soggetto pubblico, in qualità di titolare del trattamento (art. 4, comma 1, lett. *f*), del Codice), può avvalersi del contributo di soggetti esterni, anche privati (cd. *outsourcing*), affidando a essi determinate attività, che restano nella sfera della titolarità dell'amministrazione stessa, atteso che comportano decisioni di fondo sulle finalità e sulle modalità di utilizzazione dei dati. Tuttavia, in questa ipotesi, l'amministrazione pubblica titolare del trattamento deve designare il soggetto esterno come "responsabile del trattamento" con un apposito atto scritto che specifichi i compiti affidati e contenga puntuali indicazioni, anche per ciò che riguarda la sicurezza e l'utilizzo dei dati (art. 29, commi 1-5, del Codice). In caso contrario, il trattamento di dati personali si configura come una comunicazione e, in quanto tale, è assoggettata alle norme più stringenti previste per tale operazione (art. 19, comma 3, del Codice). Inoltre, è stato precisato che le persone fisiche che materialmente trattano i dati personali devono essere designate "incaricati del trattamento" con un atto scritto che individui puntualmente l'ambito del trattamento che essi possono effettuare (art. 30, comma 1, del Codice) (nota 28 maggio 2013).

In un altro caso, è stata lamentata la notificazione di una comunicazione in materia tributaria da parte di un comune, effettuata su un foglio piegato in tre parti e spillato, al cui esterno erano stati indicati dati personali eccedenti quelli strettamente necessari per la notifica (quali la data di nascita e il codice fiscale della destinataria della missiva). Il Garante ha evidenziato che i dati riguardanti la data di nascita e il codice fiscale degli interessati (ancorché utilizzati dall'Amministrazione procedente, insieme alle altre informazioni anagrafiche detenute, al fine di verificare la sussistenza di eventuali omonimie), non possono essere apposti sulla parte esterna del plico che deve riportare solo le informazioni necessarie alla notificazione della comunicazione del destinatario (cioè nome, cognome e indirizzo). Il trattamento di tali dati oggetto di segnalazione è risultato eccedente e non pertinente rispetto alla finalità perseguita di inoltrare il plico all'indirizzo delle persone cui la comunicazione è diretta, in quanto la condotta segnalata aveva comportato l'ingiustificata conoscenza delle predette informazioni da parte di terzi, in violazione dell'art. 11, comma 1, lett. *d*), del Codice. Pertanto, nel dichiarare illecito il trattamento, il Garante ha prescritto al comune di adottare per il futuro opportune cautele al fine di prevenire la conoscenza ingiustificata di dati personali eccedenti e non pertinenti da parte di soggetti terzi (provv. 18 aprile 2013, n. 201, doc. web n. 2501014).

L'Autorità, interessata in ordine alla legittimità dell'apposizione delle generalità dell'interessato sui contrassegni forniti agli agenti di commercio per l'accesso e la sosta nella zona a traffico limitato (Ztl) cittadina, in aggiunta ad un ologramma per la lettura ottica e alla targa dell'autovettura, si è espressa sulla tipologia di dati da riportare sui predetti contrassegni nel rispetto della disciplina di riferimento (che attribuisce ai comuni la facoltà di delimitare le Ztl tenendo conto degli effetti del traffico sulla sicurezza della circolazione, sulla salute, sull'ordine pubblico, sul patrimonio ambientale e culturale e sul territorio, subordinando il transito e la sosta dei veicoli, anche al servizio delle persone disabili, a particolari condizioni ai sensi degli artt. 7, comma 9, 158, 188, 198 e 201, d.lgs. 30 aprile 1992, n. 285 (Nuovo codice della strada).

Il Garante ha quindi constatato che il comune in questione, con riferimento ai contrassegni rilasciati agli "operatori di commercio e servizi", aveva previsto l'apposizione sugli stessi della ragione sociale dell'azienda che, qualora esercitata in forma di impresa individuale, deve contenere almeno la sigla o il cognome dell'imprenditore (art. 2563 c.c.), sì da identificare direttamente l'interessato (art. 4, comma 1, lett. *b*), del Codice).

Benché tali dati debbano essere utilizzati dall'amministrazione procedente al fine di rilasciare il contrassegno per il transito e la sosta nelle Ztl, la relativa indicazione sulla parte del contrassegno esposta, leggibile da chiunque, non è risultata conforme all'art. 74, commi 1 e 2, del Codice e ha comportato una diffusione di dati personali da parte di un soggetto pubblico, operazione ammessa unicamente quando è prevista da una norma di legge o di regolamento (art. 19, comma 3, Codice). Il Garante ha pertanto prescritto al comune di non apporre in futuro sulla parte dei contrassegni che devono essere esposti sui veicoli, il nome e cognome dell'interessato eventualmente contenuti nella ragione sociale dell'azienda esercitata in forma di impresa individuale, ma di indicare solo i dati riguardanti l'autorizzazione, fissando in sei mesi il termine per adempiere (provv. 24 aprile 2013, n. 217, doc. web n. 2439150).

4.10. *Le comunicazioni di dati personali tra soggetti pubblici*

Per quanto riguarda la trasmissione di dati fra soggetti pubblici l'Autorità ha risposto a un quesito del Ministero dell'interno (Dipartimento per le libertà civili e l'immigrazione - Direzione centrale per i servizi dell'immigrazione e dell'asilo) in

merito alla comunicazione di dati personali al Garante per la protezione dell'infanzia e dell'adolescenza di una regione. La questione aveva ad oggetto la richiesta di quest'ultimo di ottenere da una prefettura della regione l'elenco nominativo dei minori accompagnati dai propri genitori presenti in un Centro di accoglienza per richiedenti asilo (Cara) e di conoscere il numero complessivo delle presenze presso il Centro, suddiviso per sesso, nonché l'elenco nominativo delle donne in gravidanza. L'Autorità ha precisato che il titolare del trattamento dei dati oggetto di richiesta è tenuto a verificare l'esistenza di una norma di legge o di regolamento che ammetta la comunicazione al Garante per la protezione dell'infanzia e dell'adolescenza dei dati personali richiesti. In mancanza di una specifica normativa, con riferimento ai soli dati diversi da quelli sensibili e giudiziari, la comunicazione è altresì ammessa quando risulti comunque necessaria per lo svolgimento di funzioni istituzionali del soggetto richiedente, sempre che le modalità della comunicazione rispettino il principio di pertinenza e non determinino presso l'amministrazione ricevente un afflusso esuberante di dati rispetto alle finalità perseguite (art. 11, comma 1, lett. *d*), del Codice). In tal caso è però necessario comunicare previamente all'Autorità tale iniziativa, evidenziando le funzioni istituzionali che il Garante per la protezione dell'infanzia e dell'adolescenza è tenuto a svolgere e per le quali sarebbe necessario ottenere i dati richiesti e verificando altresì che tali funzioni siano effettivamente realizzabili unicamente attraverso l'acquisizione dei predetti dati (artt. 19, comma 3, e 39, comma 1, lett. *a*), del Codice) (nota 23 settembre 2013).

4.11. *L'attività giudiziaria*

Sicurezza nelle intercettazioni

Nella Relazione 2012 si è riferito dell'avvio da parte del Garante degli accertamenti volti a verificare l'idoneità delle misure di sicurezza adottate in relazione ai trattamenti di dati personali svolti presso le Procure della Repubblica, anche tramite la polizia giudiziaria o soggetti terzi, nell'ambito delle attività di intercettazione di conversazioni o comunicazioni, anche informatiche e telematiche, effettuate per ragioni di giustizia nonché di controllo preventivo (artt. 266 e ss. c.p.p.; art. 226 disp. att. c.p.p.). Al fine di individuare modalità operative e di cooperazione più efficaci, l'Autorità ha inoltrato una richiesta volta ad acquisire elementi conoscitivi utili da alcune Procure della Repubblica di medie dimensioni, dislocate in diverse aree del territorio nazionale e che hanno sede presso capoluoghi di provincia.

Acquisiti tali elementi, dai quali è emerso un quadro sufficientemente ampio ed esauriente delle procedure attraverso cui detti uffici acquisiscono e gestiscono le informazioni raccolte e delle misure di sicurezza adottate da ciascuna Procura, il Garante ha rilevato l'esigenza sia di realizzare alcuni interventi volti ad assicurare un rafforzamento del livello di protezione dei dati personali trattati e dei sistemi utilizzati – commisurato alla particolare importanza e delicatezza delle informazioni detenute e alla necessaria efficacia delle indagini giudiziarie nel cui ambito le intercettazioni vengono compiute –, sia di estendere l'adozione di tali interventi alla generalità degli uffici inquirenti, anche al fine di assicurare una tendenziale omogeneità delle misure e degli accorgimenti adottati.

Il Garante ha quindi prescritto alle Procure della Repubblica misure e accorgimenti, di natura sia fisica, sia informatica, per incrementare la sicurezza dei dati personali raccolti e utilizzati nello svolgimento delle intercettazioni, anche nei casi di cd. remotizzazione degli ascolti, consistente nel reindirizzamento dei flussi delle comunicazioni dai Centri intercettazioni telecomunicazioni (C.I.T.) presso le Procure verso gli uffici di polizia giudiziaria delegata (provv. 18 luglio 2013, n. 356, doc. web n. 2551507).

Ordine giudiziale di esibire i tabulati telefonici in una controversia civile

Un Tribunale ha posto al Garante un quesito relativo alla legittimità del rifiuto, opposto da parte di alcune società telefoniche, di esibire in giudizio dei tabulati telefonici a fronte della richiesta congiunta delle parti interessate e dell'ordine di esibizione dell'autorità giudiziaria in sede civile, *ex* art. 210 c.p.c. Al riguardo l'Autorità ha, in primo luogo, ricordato che, trascorso il periodo di sei mesi di conservazione dei dati per finalità di fatturazione previsto dall'art. 123 del Codice, i dati relativi al traffico telefonico possono essere conservati dal fornitore per ventiquattro mesi dalla data della comunicazione per le sole finalità di accertamento e repressione di reati, potendo essere acquisiti entro tale termine con decreto motivato del pubblico ministero, mentre il difensore dell'imputato o della persona sottoposta alle indagini può acquisire i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater* c.p.p. (art. 132 del Codice). Ciò premesso, l'Autorità ha richiamato il provvedimento generale sulla sicurezza dei dati di traffico telefonico e telematico del 17 gennaio 2008 (doc. web n. 1482111), con il quale ha precisato che il vincolo secondo cui i dati conservati obbligatoriamente per legge – per l'intervallo temporale sopra precisato (profilo da riconsiderare, unitamente ad altri non meno rilevanti, alla luce della sentenza della Corte di Giustizia dell'8 aprile 2014, *Digital Rights Ireland e Seitlinger and Others*, Cause riunite C-293/12, C-594/12, aventi ad oggetto la direttiva 2006/24/CE) – possono essere utilizzati solo per finalità di accertamento e repressione di reati comporta una precisa limitazione per i fornitori nell'eventualità in cui essi ricevano richieste volte a perseguire scopi diversi, quale quello di corrispondere a eventuali richieste riguardanti tali dati formulate nell'ambito di una controversia civile, amministrativa e contabile. Nella specie, quindi, il diniego opposto dalle società telefoniche alla richiesta di fornire i tabulati, ancorché d'ordine dell'autorità giudiziaria, ma in sede civile, *ex* art. 210 c.p.c., risulta legittimo. Il trattamento dei dati relativi al traffico telefonico – peraltro, limitatamente a quelli strettamente necessari a fini di fatturazione – è ammesso in sede civile solamente per controversie attinenti alla fattura telefonica.

Trattamento di dati sensibili e giudiziari a fini di ricerca scientifica

Un ufficio periferico del Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia ha posto un quesito attinente alla legittimità della comunicazione ad una università, sulla base di un protocollo sottoscritto dalle parti e per finalità di ricerca, di dati sensibili e giudiziari di soggetti condannati ammessi all'esecuzione penale esterna. L'Autorità, premesso che, in tali casi, occorre previamente valutare se, ai fini della ricerca scientifica, non sia sufficiente il trattamento di dati anonimi, ha ricordato che il trattamento dei dati personali effettuato per scopi statistici e scientifici è regolato dagli artt. 104-110 del Codice e dalle disposizioni del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (provv. 16 giugno 2004, n. 2, doc. web n. 1556635) – tra le quali assumono particolare rilievo quelle dettate dall'art. 9 – il cui rispetto costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati (art. 12 del Codice) (nota 18 aprile 2013).

Accesso ad atti di procedura di affidamento

Nel fornire riscontro ad una segnalante che lamentava il mancato rilascio da parte di un'assistente sociale di documenti relativi alla procedura di affidamento di sua figlia, l'Ufficio ha rilevato che la questione non rientra nella competenza del Garante (v. in argomento *supra* par. 4.3). Ove, infatti, si tratti di atti amministrativi, attesa la distinzione fra diritto di accesso ai dati personali e diritto di accesso agli atti ed ai documenti amministrativi di cui alla l. n. 241/1990, il rifiuto del destinatario a consentire l'accesso può essere oggetto di istanza di riesame avanti alla Commissione per l'accesso ai documenti amministrativi o di impugnazione avanti al competente tribunale amministrativo regionale. Ove, invece, si tratti di atti che fanno parte di un procedimento giudiziario – in quanto nella segnalazione veniva riferito che la procedura era gestita

da un tribunale per i minorenni – ogni doglianza sul comportamento dell'assistente sociale, ivi compreso il negato rilascio degli atti, deve essere sottoposta alla competente autorità giudiziaria (nota 17 ottobre 2013).

Pubblicità dei dati nei procedimenti di espropriazione forzata

Anche nel 2013 sono pervenute all'Autorità segnalazioni relative al regime di pubblicità nell'ambito dei procedimenti di espropriazione forzata introdotto dalla riforma del processo esecutivo (d.l. 14 marzo 2005, n. 35, convertito, con modificazioni, dalla l. 14 maggio 2005, n. 80), che prevede la pubblicazione su appositi siti internet di copia dell'ordinanza del giudice che dispone sulla vendita forzata e della relazione di stima dei beni da espropriare.

Diffusione di avvisi d'asta

Sul tema è stato presentato un quesito con cui si è chiesto di conoscere se sia legittimo, come accaduto nel caso segnalato, che negli avvisi d'asta pubblicati nei quotidiani e nei siti internet dei vari tribunali siano contenute molteplici informazioni concernenti gli immobili posti all'asta, tenuto conto che chiunque, tramite detta pubblicità, può individuare l'interessato di cui conosca l'indirizzo di abitazione. Al riguardo, il Garante ha evidenziato che la normativa in materia di aste giudiziarie prevede, tra l'altro, la pubblicità degli avvisi d'asta, contenenti ogni informazione ritenuta utile e necessaria a descrivere gli immobili al fine del corretto espletamento della procedura di vendita, con l'omissione dell'indicazione del debitore (art. 490 c.p.c., come modificato dall'art. 174, comma 9, del Codice). Tenuto conto di ciò, con provvedimento generale del 7 febbraio 2008 (doc. web n. 1490838) il Garante ha invitato gli uffici giudiziari e i professionisti delegati alle operazioni di vendita nelle esecuzioni immobiliari ad applicare le vigenti disposizioni del codice di rito, sottolineando la necessità di omettere l'indicazione del debitore e di eventuali terzi estranei alla procedura dagli avvisi d'asta e dalla documentazione ad essi allegata. L'Ufficio ha quindi evidenziato che nell'ipotesi in cui, come nella specie, venga rispettata la prescrizione che impone di omettere l'indicazione del debitore, la pubblicità delle informazioni, anche dettagliate, concernenti gli immobili posti all'asta risulta conforme alla normativa di settore, nonché lecita sotto il profilo della disciplina in materia di protezione dei dati personali, e più specificatamente del principio di pertinenza e non eccedenza dei dati (art. 11, comma 1, lett. *d*), del Codice) (nota 5 settembre 2013).

4.11.1. L'informatica giuridica

Pubblicazione di sentenze a fini di informazione giuridica

Con riferimento alla segnalazione concernente la pubblicazione di una sentenza sul sito web di un ufficio giudiziario, recante l'indicazione in chiaro del nominativo del segnalante, l'Ufficio, nel richiamare le "Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica", adottate dal Garante il 2 dicembre 2010 (doc. web n. 1774813), ha ricordato che il Codice prevede all'art. 52 una specifica procedura, avviata ad istanza dell'interessato prima che sia definito il relativo grado di giudizio con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede (commi 1 - 4), per omettere i dati personali sulle sentenze e sugli altri provvedimenti giudiziari pubblicati per finalità di informazione giuridica. L'Autorità ha aggiunto che l'anonimizzazione delle pronunce è imposta dalla legge per i dati concernenti l'identità di minori oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone (comma 5). Eccettuati i suddetti casi, il Codice ammette la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali (comma 7) (nota 7 ottobre 2013).

Il Garante per l'infanzia e l'adolescenza di una regione e l'Associazione nazionale famiglie adottive e affidatarie hanno segnalato che in una rivista di informazione giuridica era stata pubblicata *online* una sentenza di un Tribunale per i minorenni emessa in un procedimento in materia di adottabilità di una minore, in versione

integrale, ovvero recante in chiaro il nominativo della minore e altri dati idonei ad identificarla, ivi compresi il luogo e la data di nascita e il nome della madre. L'Autorità, nel chiedere al gestore della rivista l'immediata anonimizzazione della sentenza, mediante l'omissione di ogni dato dal quale poteva desumersi, anche indirettamente, l'identità della minore nonché della madre, della quale veniva riportato l'episodio di una violenza sessuale, ha ricordato i divieti di diffondere dati da cui possa desumersi anche indirettamente l'identità di minori (art. 52, comma 5, del Codice) e le generalità delle persone offese (tra l'altro) da atti di violenza sessuale senza il loro consenso (art. 734-*bis* c.p., richiamato anche dal citato comma 5 dell'art. 52) (nota 5 settembre 2013).

Con successiva nota l'Autorità ha preso atto della espunzione della sentenza dal sito della rivista, ricordando altresì che l'anonimizzazione deve essere curata anche con riferimento alle eventuali massime estratte dai provvedimenti giurisdizionali, che non devono contenere informazioni dalle quali sia possibile risalire all'identità dei soggetti tutelati (nota 17 settembre 2013).

4.11.2. Le notificazioni di atti e comunicazioni

Nel 2013 sono pervenute diverse segnalazioni circa le modalità di notificazione di atti giudiziari in modo non conforme alle prescrizioni del Codice.

Notificazioni di atti giudiziari a mezzo posta

In una segnalazione si è lamentato che sulla busta di notificazione di un atto giudiziario destinato al segnalante e proveniente da uno studio legale, era stata apposta la dicitura "a mani proprie perché è una separazione x il portalettere".

L'Ufficio notifiche della Corte d'appello competente ha rappresentato che era consuetudine dell'ufficio, per la mole di lavoro e la carenza di personale, ricevere atti per la notificazione a mezzo del servizio postale già completi di busta e cartolina verde precompilati dai richiedenti e che, nella specie, la busta era stata già compilata con tutte le diciture a cura di un ufficio legale. Al riguardo l'Ufficio ha evidenziato che la normativa di settore in tema di notifiche di atti giudiziari affida all'ufficiale giudiziario, se non è disposto altrimenti, il compito di eseguire le notificazioni (art. 137 c.p.c.) e, quando queste vengono effettuate a mezzo posta, gli ufficiali giudiziari devono fare uso di speciali buste sulle quali non sono apposti segni o indicazioni dai quali possa desumersi il contenuto dell'atto (art. 2, l. n. 890/1982, come modificato dall'art. 174 del Codice). Si è pertanto ritenuto che l'ordinamento giuridico affida all'ufficiale giudiziario il compito e la responsabilità, anche al fine del risarcimento dell'eventuale danno provocato dal non corretto trattamento dei dati, di curare gli adempimenti relativi alla notificazione di atti giudiziari, e che non assume rilievo la circostanza che l'indirizzamento sulla busta sia predisposto da altri (nota 16 gennaio 2013).

Notificazioni di atti giudiziari presso il luogo di lavoro

Un cittadino ha segnalato di avere ricevuto, nell'ambito di alcuni procedimenti penali che lo vedono coinvolto a vario titolo, notifiche di atti giudiziari da parte di una Procura della Repubblica presso il luogo di lavoro, anziché al domicilio eletto presso il proprio difensore, con la conseguenza della conoscenza del contenuto degli atti da parte di un numero di soggetti maggiore di quelli che sarebbero stati coinvolti nel caso in cui la notifica fosse stata effettuata presso il domicilio eletto. Effettuate le necessarie verifiche, l'Autorità ha rilevato che anche i trattamenti effettuati per ragioni di giustizia debbono rispettare il principio posto dall'art. 11 del Codice relativo alla non eccedenza del trattamento rispetto alle finalità per le quali i dati personali sono raccolti o successivamente trattati. La disciplina legale delle forme di notifica di atti giudiziari, come pure modificata dal Codice (art. 174), garantisce la tutela della riservatezza dei dati personali, unitamente all'esigenza di assicurare lo svolgimento delle funzioni giudiziarie. Poiché nella vicenda risultava che, in un caso, la

notifica di atti giudiziari, per mera svista, anziché presso il domicilio eletto presso il difensore era, invece, stata effettuata all'interessato attraverso consegna a mani proprie, determinando il coinvolgimento nel trattamento dei dati personali del segnalante anche gli organi di polizia giudiziaria della località di notifica, l'Ufficio ha ritenuto il descritto trattamento, senza che specifiche ed oggettive esigenze processuali lo richiedessero, non in linea con il canone della non eccedenza rispetto alle finalità del trattamento stesso (art. 11 del Codice). È stata quindi richiamata l'attenzione degli uffici giudiziari interessati sul rispetto delle norme del Codice, oltre che di quelle processuali in materia di notifica degli atti giudiziari, al fine della miglior tutela della riservatezza dei destinatari (nota 23 settembre 2013).

5 La sanità

5.1. *I trattamenti per fini di cura della salute*

Il trattamento dei dati personali effettuato da parte di soggetti pubblici e privati per finalità di prevenzione, diagnosi, cura e riabilitazione dell'interessato continua a formare oggetto di specifica attenzione da parte dell'Autorità.

A seguito di notizie stampa, l'Autorità è intervenuta in un caso in cui un assessore alla tutela della salute aveva inviato una *e-mail* a tutte le donne che si erano rivolte alla sua segreteria per protestare contro la chiusura di un centro specializzato nella cura delle patologie tumorali della mammella al fine di spiegare la scelta di riconversione del suddetto presidio sanitario. Analogamente ai casi già affrontati nel 2012, la suddetta *e-mail* era stata inviata inserendo gli indirizzi delle donne in un campo visibile a tutti i destinatari della comunicazione. In tal modo, i destinatari della *e-mail* erano venuti a conoscenza dei nominativi di tutte le pazienti che afferivano al centro oncologico. A seguito dell'intervento del Garante, l'assessore ha riconosciuto il proprio errore e ha attivato iniziative per evitare il ripetersi di tali incidenti. Sul caso l'Autorità ha avviato un procedimento sanzionatorio circa l'avvenuta comunicazione a terzi di dati idonei a rivelare lo stato di salute senza il consenso degli interessati, che si è concluso con il pagamento della sanzione da parte del contravventore (note 19 dicembre 2012 e 5 marzo 2013).

L'Ufficio è altresì intervenuto in un caso in cui un medico aveva inviato al proprio assistito una perizia legata ad una causa di risarcimento del danno attraverso un indirizzo *e-mail* istituzionale assegnato ad una collega. A seguito dell'intervento dell'Autorità, che ha avviato un procedimento sanzionatorio, l'azienda sanitaria ove era impiegata la collega del medico che aveva redatto la perizia ha provveduto alla cancellazione e distruzione dei dati relativi al segnalante (nota 21 giugno 2013).

Emerso da notizie stampa che alcuni pazienti di un laboratorio di analisi avevano ricevuto telefonate con le quali venivano invitati ad esprimere la propria preferenza nei confronti di un medico operante nel laboratorio nelle imminenti consultazioni elettorali, l'Autorità ha ricordato che quando si presta un'attività o un servizio presso una struttura sanitaria non è lecito utilizzare indirizzari o altri dati personali per finalità incompatibili con quelle che ne avevano giustificato la raccolta, nel caso di specie propagandare candidati interni alla struttura o da questa sostenuti. Gli indirizzari trattati per svolgere le attività del medico o della struttura sanitaria non possono essere di per sé utilizzati per fini elettorali, essendo stati raccolti per fini di cura della salute dell'interessato (nota 21 giugno 2013 e già provv.ti 12 febbraio 2004, doc. web n. 634369 e 7 settembre 2005, doc. web n. 1165613).

In una fattispecie analoga, a seguito di una segnalazione di un paziente che, dopo aver eseguito una visita urologica presso una struttura sanitaria italiana, aveva ricevuto comunicazioni di carattere commerciale da parte di una società residente a San Marino (avente ad oggetto un prodotto fitoterapico per la cura di alcuni disturbi urinari), l'Autorità ha interessato il Garante per la tutela della riservatezza sammarinese (nota 28 febbraio 2013).

Non diversamente, l'Ufficio è intervenuto a seguito della segnalazione presentata da alcuni pazienti di un'azienda sanitaria che lamentavano di aver ricevuto

dalla stessa un test di valutazione di incontinenza urinaria da compilare per consentire all'azienda di ottimizzare la scelta dei presidi sanitari da distribuire agli stessi. In tale attività sono risultati coinvolti soggetti esterni all'azienda sanitaria operanti nel campo della riabilitazione e della fornitura di prodotti per incontinenti. L'azienda, a seguito dei rilievi formulati dall'Autorità in ordine al ruolo ricoperto da tali soggetti e alle finalità di tale trattamento, ha sospeso l'iniziativa (note 11 dicembre 2012 e 3 maggio 2013).

L'Ufficio è intervenuto, avviando un procedimento sanzionatorio, con riguardo al comportamento, segnalato dalla stampa, tenuto da un medico dentista che aveva affisso sul bancone del proprio studio l'elenco nominativo dei pazienti morosi. L'elenco è stato tempestivamente rimosso (nota 20 giugno 2013).

L'Autorità è stata chiamata ad esprimersi in merito alla possibilità che gli organismi sanitari, in occasione dello svolgimento di analisi delle urine in capo a particolari categorie di lavoratori per accertarne l'eventuale stato di tossicodipendenza, possano usare sistemi di videosorveglianza all'interno dei propri servizi igienici. Tale esigenza nasce dalla circostanza che i lavoratori destinati a mansioni che comportano rischi per la sicurezza, l'incolumità e la salute di terzi devono essere sottoposti per legge, prima dell'assunzione in servizio e poi con cadenza periodica, ad un accertamento circa l'assenza di tossicodipendenza attraverso l'esame delle urine. I medesimi accertamenti devono essere effettuati anche nei confronti dei soggetti affetti da dipendenze per finalità di cura. Poiché nell'ambito di tali accertamenti le strutture sanitarie devono assicurare una correlazione univoca tra il campione urinario e il soggetto sottoposto ad accertamento, le procedure in atto prevedono che il soggetto non possa essere lasciato solo durante la raccolta del campione urinario, ma sia osservato da un operatore sanitario qualificato.

Alla luce dell'esperienza maturata, le strutture sanitarie hanno rilevato la necessità, in luogo dell'osservazione diretta da parte dell'operatore sanitario, dell'impiego di sistemi di videosorveglianza al fine di assicurare la corretta raccolta – sotto il profilo dell'inalterabilità e della provenienza – del campione urinario del soggetto obbligato ai fini di legge all'accertamento. Infatti, in molteplici casi, le persone sottoposte ad accertamento avevano manifestato il proprio disagio nel raccogliere il campione urinario sotto la diretta osservazione di un operatore sanitario. Con un provvedimento a carattere generale l'Autorità ha ritenuto che debba essere riconosciuta all'interessato la facoltà di scegliere se consentire l'osservazione diretta di un operatore sanitario o la rilevazione delle immagini che lo riguardano attraverso sistemi di videosorveglianza. In quest'ultima ipotesi, le immagini rilevate non devono essere registrabili ed il servizio igienico dotato di telecamere deve essere dedicato in via esclusiva all'esecuzione di tali controlli. Ove ciò non sia possibile, devono essere introdotti opportuni accorgimenti per evitare l'esecuzione di riprese in casi non previsti. Infine, il personale sanitario preposto ai controlli – il solo abilitato a visionare le immagini e preferibilmente dello stesso sesso della persona da controllare – deve essere designato per iscritto incaricato del trattamento e deve essere preclusa la possibilità di registrare le immagini che appaiono sullo schermo, anche tramite telefoni cellulari o altri dispositivi elettronici (provv. 15 maggio 2013, n. 243, doc. web n. 2475383).

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

L'Autorità ha continuato ad occuparsi delle modalità con cui le strutture sanitarie pubbliche e private forniscono l'informativa agli interessati e acquisiscono il loro consenso per i trattamenti di dati personali necessari ai fini di cura.

A seguito di una segnalazione, l'Autorità è intervenuta in un caso in cui uno psicanalista aveva prestato le proprie cure ad una paziente senza aver acquisito dalla stessa

il consenso al trattamento dei suoi dati personali. Nell'ambito dell'istruttoria è emerso, inoltre, che il medico aveva anche comunicato informazioni relative al delicato stato di salute della segnalante a terzi senza averne acquisito il consenso. In merito a tali aspetti è stato avviato un procedimento sanzionatorio che si è concluso con il pagamento da parte del contravventore (nota 25 luglio 2013).

Tra le diverse questioni esaminate merita di essere menzionata la segnalazione di una neuropsichiatra infantile in merito all'iniziativa di un azienda sanitaria di far condividere l'elenco nominativo dei bambini presi in carico tra i diversi servizi di neuropsichiatria infantile distrettuali al fine di evitare duplicazioni e sovrapposizioni nell'erogazione delle prestazioni sanitarie.

L'Autorità ha provveduto a richiedere informazioni all'azienda sanitaria in merito a tale vicenda, evidenziando che qualora il titolare del trattamento intenda comunicare dati sensibili per fini di cura a soggetti diversi dall'interessato, in assenza di una disposizione normativa al riguardo, deve richiedere uno specifico consenso informato a quest'ultimo; nel caso in cui l'interessato sia incapace di intendere o volere, il consenso dovrà essere manifestato da parte del legale rappresentante. Pertanto, il servizio di neuropsichiatria infantile che intenda procedere alla comunicazione ad altro analogo servizio dell'elenco nominativo dei minori presi in cura deve acquisire uno specifico consenso informato dell'interessato (o di chi ne fa le veci), anche nel rispetto del rapporto fiduciario instauratasi tra medico e paziente nonché della legittima volontà dell'interessato di richiedere il parere di un altro specialista (nota 9 ottobre 2013).

L'Autorità ha preso in considerazione, anche mediante attività ispettive, le questioni legate alla necessaria specificità del contenuto dell'informativa rispetto ai trattamenti di dati personali effettuati in particolari ambiti sanitari (es. pronto soccorso, ricoveri). In particolare, specifici approfondimenti sono stati posti in essere con riferimento ai trattamenti effettuati, avuto riguardo alle molteplici finalità perseguite (di cura, amministrative e commerciali), dalle strutture termali.

5.1.2. Il Fascicolo sanitario elettronico e i dossier sanitari

Costante è stata l'attenzione nei confronti delle problematiche legate alla realizzazione a livello nazionale del Fascicolo sanitario elettronico (Fse), disciplinato con il d.l. 18 ottobre 2012, n. 179 (Ulteriori misure urgenti per la crescita del Paese) convertito dalla l. 17 dicembre 2012, n. 221 (art. 12). L'impianto normativo definisce il Fse e riconosce la centralità del consenso dell'interessato per la sua costituzione secondo una prospettiva corrispondente a quella elaborata dall'Autorità nelle "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di *dossier* sanitario" (provv. 16 luglio 2009, doc. web n. 1634116).

In tale cornice, l'Autorità ha partecipato al tavolo di lavoro istituito presso il Ministero della salute ai fini dell'emanazione del decreto di attuazione del Fse in cui devono essere individuati, tra l'altro, i contenuti del Fse, le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali, i sistemi di codifica dei dati, le modalità e i livelli diversificati di accesso al Fse, la definizione e le relative modalità di attribuzione di un codice identificativo univoco dell'assistito che non consenta l'identificazione diretta dell'interessato. Nell'ambito delle attività svolte nel suddetto tavolo di lavoro, l'Autorità ha formulato numerose osservazioni con specifico riferimento al perseguimento di finalità ulteriori rispetto a quella di cura dell'interessato riconducibili a quelle di ricerca scientifica e di governo, nonché relativamente al diritto di oscuramento dei dati e al rispetto di elevati *standard* di sicurezza sia fisica che logica al fine di consentire l'accesso ai dati sanitari solo da parte del personale a ciò autorizzato. La bozza di decreto elaborata dal tavolo di lavoro è all'esame della Presidenza del Consiglio dei Ministri.

In merito all'utilizzo dei *dossier* sanitari da parte delle strutture sanitarie sono state avviate diverse istruttorie, sia d'ufficio che a seguito di specifiche segnalazioni, al fine di verificare se i sistemi attualmente in uso rispettino le misure indicate dal Garante nelle citate linee guida. In tale provvedimento il Garante ha considerato quale *dossier* sanitario lo strumento costituito presso un organismo sanitario in qualità di unico titolare del trattamento al cui interno operino più professionisti (es., ospedale o azienda sanitaria), contenente informazioni inerenti allo stato di salute di un individuo relative ad eventi clinici presenti e trascorsi (es.: referti, documentazione relativa a ricoveri, accessi al pronto soccorso) volte a documentarne la storia clinica.

Le istruttorie avviate hanno coinvolto in particolar modo alcune strutture sanitarie pubbliche interessate da accertamenti ispettivi. I principali aspetti su cui si è concentrato l'intervento dell'Ufficio hanno riguardato le soluzioni adottate dalle diverse strutture sanitarie affinché l'accesso al *dossier* sia consentito ai soli professionisti sanitari che hanno attualmente in cura il paziente (note 12 e 18 dicembre 2013 nonché 27 gennaio 2014).

Con specifico riferimento all'esigenza di limitare l'accesso al *dossier* sanitario da parte del personale non sanitario operante nelle strutture assistenziali, merita evidenziare che a seguito dell'intervento dell'Autorità, un'azienda per i servizi alla persona ha modificato i parametri di accesso al proprio *dossier* sanitario consentendo al solo personale che ha in cura i pazienti di visualizzarne le informazioni sanitarie (nota 28 febbraio 2013). Prima dell'intervento dell'Autorità tale accesso era consentito anche al personale amministrativo e di direzione gestionale dell'azienda.

Accesso al *dossier* sanitario

Come descritto nella Relazione 2012, con specifico riferimento all'utilizzo del *dossier* sanitario, l'Autorità ha effettuato un importante accertamento ispettivo nei confronti delle strutture sanitarie pubbliche di una regione, all'esito del quale ha adottato un provvedimento nei confronti di tutte le strutture sanitarie pubbliche regionali prescrivendo alle stesse le misure da adottare al fine di prevenire indebiti accessi da parte del personale sanitario ai *dossier* dei pazienti ove non sia in corso una prestazione sanitaria (provv. 10 gennaio 2013, n. 3, doc. web n. 2284708).

Le misure prescritte dal Garante hanno avuto un forte impatto sulla gestione dei servizi informativi sanitari della Regione che ha dovuto implementare misure logiche e informatiche affinché i documenti sanitari trattati attraverso lo strumento del *dossier* sanitario restino disponibili solo al professionista che ha attualmente in cura il paziente (e non siano pertanto più automaticamente condivisi con altri professionisti che non lo abbiano in cura).

Considerata la complessità e l'eterogeneità dell'intero sistema informativo regionale e la necessità che le modifiche necessarie per ottemperare al provvedimento dell'Autorità siano adeguatamente testate dal punto di vista tecnico-organizzativo, al fine di garantire la corretta operatività della gestione del processo di cura, il Garante ha concesso una proroga dei termini ivi previsti per una graduale adozione delle misure prescritte, mantenendo una vigilanza sullo stato di introduzione delle modifiche al sistema informativo sanitario regionale (provv. 22 maggio 2013, n. 252, doc. web n. 2550110 e provv. 1° agosto 2013, n. 381, doc. web n. 3060291). Tali proroghe sono state concesse dopo aver verificato che molte delle prescrizioni erano state già adottate e che altre erano in corso di attuazione; in tali provvedimenti il Garante ha altresì individuato un termine finale (fissato al 30 marzo 2014) per ottemperare a quanto disposto nel citato provvedimento del 10 gennaio 2013.

Successivamente all'adozione di tali provvedimenti, l'Autorità ha continuato a ricevere segnalazioni in merito a casi di accessi abusivi al sistema informativo utilizzato dalle strutture sanitarie della Regione da parte del personale ivi operante. Alcune delle istruttorie sono tuttora in corso. I casi segnalati riguardano accessi a dati sanitari di

pazienti delle strutture sanitarie da parte di medici che avevano preso conoscenza dei dati per finalità per lo più personali e comunque non legate alla cura degli interessati (note 27 febbraio 2013, 24 marzo 2013 e 18 dicembre 2013). Nei casi segnalati gli accessi abusivi sono risultati effettuati prima che il Garante adottasse il richiamato provvedimento del 10 gennaio 2013. Nelle istruttorie avviate dall'Ufficio, è emerso, infatti, che a seguito del suddetto provvedimento, oltre ad un processo di revisione delle caratteristiche del sistema informativo sanitario regionale, è stato effettuato anche un significativo intervento di sensibilizzazione nei confronti del personale sanitario in merito al rispetto delle garanzie in materia di protezione dei dati personali già richiamate dal Garante nelle linee guida del 2009.

5.1.3. I referti e la documentazione sanitaria

Viene frequentemente segnalata la consegna di referti a soggetti diversi dall'interessato in busta aperta o senza verificare l'esistenza della delega per il ritiro degli stessi. A tal proposito l'Ufficio ha ricordato che le certificazioni rilasciate dagli organismi sanitari possono essere ritirate anche da persone diverse dai diretti interessati dopo aver verificato l'identità del soggetto a ciò delegato sulla base di idonei elementi (ad es., mediante l'esibizione di un documento di riconoscimento) e mediante la consegna delle stesse in busta chiusa (note 4 e 27 febbraio 2013 nonché 2 aprile 2013). A seguito di tali interventi le aziende sanitarie interessate hanno modificato le procedure per la consegna dei referti in conformità a quanto indicato dall'Autorità.

Un procedimento sanzionatorio è stato avviato a seguito della consegna di una cartella clinica relativa al ricovero di un minore ad una persona sprovvista di delega per il ritito e rimasta sconosciuta. L'azienda sanitaria, riconosciuto il proprio errore, a seguito dell'intervento dell'Ufficio (che ha avviato un procedimento sanzionatorio) ha provveduto a sensibilizzare il personale dell'ufficio cartelle cliniche al rispetto delle regole relative alla consegna della documentazione sanitaria (nota 30 settembre 2013).

L'Ufficio è anche intervenuto in merito alle modalità di custodia delle prescrizioni mediche da parte di alcuni pediatri in attesa del loro ritiro da parte dei genitori. Nei casi esaminati le prescrizioni venivano collocate in contenitori non custoditi o affisse nelle bacheche situate nella sala di attesa dello studio medico. L'Ufficio ha rappresentato che devono essere adottate idonee cautele per evitare che le informazioni sanitarie possano essere conosciute da terzi (nel caso di specie, i pazienti presenti in sala di attesa o quelli che erroneamente ritirino una prescrizione non propria) e che il personale designato incaricato del trattamento (ad es., il personale di segreteria) deve essere debitamente istruito in ordine alle modalità di consegna dei documenti contenenti dati idonei a rivelare lo stato di salute (note 5 giugno 2013 e 7 novembre 2013). I medici interessati hanno prontamente modificato la prassi di consegna delle prescrizioni con procedure conformi alle indicazioni dell'Autorità.

Già nel 2009, l'Autorità si era occupata di definire un quadro unitario di garanzie nei confronti dei servizi offerti da numerose strutture sanitarie per ricevere i referti via posta elettronica o per consultarli telematicamente sul sito web della struttura sanitaria (Linee guida in tema di referti *online*, provv. 19 novembre 2009, doc. web n. 1679033). Al riguardo, a seguito di alcune segnalazioni, sono stati avviati accertamenti nei confronti di un'azienda sanitaria locale, al fine di verificare il rispetto delle misure a tutela dei dati personali individuate nelle citate linee guida (nota 22 ottobre 2013).

A seguito di una pluralità di segnalazioni concernenti servizi offerti attraverso il cd. Sportello Amico di Poste Italiane, con particolare riferimento a quelli relativi al pagamento del *ticket* e al ritiro dei referti, l'Ufficio ha aperto un'istruttoria, anche mediante accertamenti ispettivi, per verificare il rispetto delle misure a tutela dei dati personali (nota 23 ottobre 2013).

L'Autorità è intervenuta nei casi, spesso segnalati dagli organi di stampa, di abbandono della documentazione sanitaria in locali in disuso accessibili al pubblico. In tali casi, le aziende sanitarie coinvolte hanno provveduto a rimuovere la documentazione sanitaria e ad adottare le misure di sicurezza previste dal Codice e dall'Allegato tecnico in merito alla conservazione della documentazione, anche in conformità a quanto previsto dalla disciplina sugli Archivi di Stato (nota 28 marzo 2013).

Hanno formato oggetto di segnalazione casi in cui l'interessato aveva ricevuto, oltre alla propria documentazione sanitaria, anche quella relativa ad altre persone. In un caso, all'esito di un ricovero era stata consegnata ad un paziente documentazione riguardante informazioni sanitarie di terzi. Tale circostanza, pur se dipesa da un errore, ha determinato un'illegittima comunicazione di dati sanitari di numerosi pazienti, con conseguente avvio di un procedimento sanzionatorio (nota 2 aprile 2013). In un altro caso, un centro psicosociale aveva consegnato ad un paziente l'elenco dei soggetti nei cui confronti il Dipartimento di salute mentale aveva disposto un trattamento sanitario obbligatorio. L'errore, dovuto all'inserimento di tale documento in un fax (che pure ha determinato anche in tal caso l'attivazione di un procedimento sanzionatorio), è stato ammesso dalla struttura sanitaria che ha modificato la prassi utilizzata per l'invio di documenti sanitari tra le diverse sedi e ha adottato opportune misure per evitare che si ripetano fatti analoghi a quelli segnalati (nota 12 aprile 2013).

5.1.4. La tutela della dignità della persona

Gli interventi dell'Autorità in ambito sanitario – come già accaduto – sono volti a garantire, da un lato, il rispetto delle disposizioni in materia di protezione di una delicata categoria di dati personali afferenti alla salute dell'interessato nonché, dall'altro, a tutelare la dignità dei pazienti nell'ambito del loro percorso di cura (artt. 2 e 83 del Codice).

Un quadro generale delle misure che devono essere adottate da parte delle strutture sanitarie per garantire la dignità dei pazienti era stato già fornito con il provvedimento generale del 9 novembre 2005 (doc. web n. 1191411).

A seguito delle numerose segnalazioni ricevute in merito alle modalità con cui le aziende sanitarie – anche per il tramite di società operanti in *outsourcing* – effettuano la consegna dei presìdi sanitari al domicilio degli interessati, l'Autorità ha ritenuto opportuno integrare il suddetto provvedimento del 2005, prescrivendo a tutte le strutture sanitarie di adeguare – entro giugno 2015 – le operazioni di consegna domiciliare dei presìdi sanitari alle misure indicate nel provvedimento. Le segnalazioni ricevute lamentavano le modalità di consegna di specifici presìdi, quali quelli utilizzati da persone incontinenti o stomizzate (ad es., cateteri, ausili per evacuazione e per stomia, raccoglitori e assorbenti per urina), recapitati in pacchi trasparenti o recanti sulla parte esterna o sulla bolla di consegna l'indicazione in chiaro della tipologia del contenuto, ovvero consegnati al vicino di casa o al portiere, in assenza di autorizzazione dell'interessato; in taluni casi, i predetti presìdi sarebbero stati lasciati incustoditi davanti la porta di ingresso della dimora dell'interessato.

Al fine di porre rimedio a tale condotta il Garante ha individuato alcune misure da osservare nelle operazioni di consegna. In primo luogo, essa deve avvenire preferibilmente nelle mani dell'interessato rispettando gli orari scelti da quest'ultimo tra quelli indicati dal titolare; il presidio non può essere lasciato incustodito nelle vicinanze del luogo indicato dall'interessato; nel caso in cui quest'ultimo non sia presente al momento della consegna, il personale a ciò deputato deve lasciare esclusivamente un avviso privo dell'indicazione della tipologia del presidio. Il presidio deve essere imballato in un contenitore non trasparente sprovvisto di indicazione circa il suo contenuto; può essere consegnato a terzi (ad es., vicino di casa, parente, portiere) solo

su espressa indicazione dell'interessato; il personale deputato alla consegna non deve indossare divise recanti scritte da cui si possa evincere la specifica tipologia dei presìdi in consegna, né utilizzare automezzi recanti tali scritte (provv. 21 novembre 2013, n. 520, doc. web n. 2803050).

In proposito l'Ufficio è intervenuto in un caso in cui un paziente aveva segnalato che la struttura sanitaria distrettuale aveva consegnato al portiere del proprio stabile un pacco recante all'esterno l'indicazione della tipologia del contenuto (prodotti per l'incontinenza), senza che l'interessato avesse delegato il portiere a ritirare tali presìdi. A seguito di tale intervento (che ha determinato l'attivazione di un procedimento sanzionatorio) la società incaricata della consegna ha accertato che il proprio dipendente non aveva rispettato le procedure aziendali circa la consegna dei presìdi e lo ha sottoposto ad un provvedimento disciplinare (nota 8 ottobre 2013).

Il richiamo al rispetto della dignità dei pazienti è stato più volte necessario in merito alle condizioni con cui vengono prestate le cure in numerosi ospedali italiani. Al riguardo, l'Ufficio ha ricordato che le strutture sanitarie devono organizzare la prestazione dei servizi adottando opportuni accorgimenti a tutela delle libertà fondamentali e della dignità dei pazienti (ad es., per limitare la visibilità dell'interessato durante la visita o per evitare che in tali occasioni le informazioni sulla sua salute possano essere conosciute da terzi) (note 9 gennaio e 1° ottobre 2013).

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

Con particolare riferimento alla delicatissima materia del trattamento dei dati personali effettuato nell'ambito dell'erogazione delle prestazioni mediche a pazienti affetti da HIV, sono pervenute alcune segnalazioni con riferimento all'esibizione del codice di esenzione dalla partecipazione al costo per le prestazioni di assistenza sanitaria previsto per le infezioni da HIV. Alcuni interessati, specie se residenti in piccoli centri, lamentano inoltre di dover effettuare le pratiche amministrative per il rilascio o il rinnovo dell'esenzione da HIV nella propria Asl di residenza, ove spesso è impiegato personale che, per le ragioni più varie, può avere conoscenza diretta dei pazienti.

In merito a tali profili, si è ritenuto opportuno avviare un confronto con il Ministero della salute - Direzione generale della programmazione sanitaria e l'Istituto Superiore di Sanità (ISS) - Dipartimento malattie infettive parassitarie e immunomediate, al fine di valutare la possibilità di individuare idonee cautele volte a non far evincere in modo immediato l'esistenza di un'infezione da HIV attraverso la mera presentazione del codice di esenzione all'atto della prenotazione o della prestazione sanitaria, nonché di individuare percorsi alternativi a quello previsto dalla legge per espletare le pratiche di rilascio o rinnovo dell'esenzione (nota 11 aprile 2013).

Con specifico riferimento alle questioni sopra descritte, l'Ufficio ha avviato un'istruttoria in merito alle procedure di riconoscimento dell'esenzione per la menzionata patologia in uso presso una Regione. Nel caso sottoposto all'attenzione dell'Ufficio l'interessato affetto da HIV, in quanto dipendente della propria Asl di residenza, segnalava una violazione della propria riservatezza nel dover avviare le pratiche amministrative per il riconoscimento del diritto all'esenzione per patologia in un ambiente che coincideva con quello lavorativo. Successivamente all'intervento dell'Ufficio (nota 15 gennaio 2013), la Giunta regionale ha adottato linee guida in cui si invitano le aziende sanitarie a mettere in atto una procedura che consenta agli operatori dei reparti di malattie infettive di provvedere, su richiesta del paziente, ad espletare le pratiche di esenzione presso l'azienda sanitaria di residenza dell'assistito senza che lo stesso sia costretto a presentarsi direttamente agli sportelli amministrativi che sono di norma tenuti ad accogliere le richieste di esenzione.

A seguito di una segnalazione, il Garante è tornato ad occuparsi della raccolta delle informazioni legate alla sieropositività dei pazienti che si recano presso gli studi dentistici. Già nel 2009, con un provvedimento generale, il Garante aveva prescritto agli esercenti le professioni sanitarie di non 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, e a prescindere dal tipo di intervento o piano terapeutico da eseguire, fermo restando che tale dato anamnestico poteva essere legittimamente raccolto, previo consenso informato dell'interessato, da parte del medico curante nell'ambito del processo di cura, in relazione a specifici interventi clinici ove ciò sia ritenuto necessario (provv. 12 novembre 2009, doc. web n. 1673588).

In una segnalazione un dentista invitava i propri pazienti a compilare una scheda anamnestica in cui veniva richiesto, tra l'altro, se gli stessi fossero affetti da HIV. Al riguardo, l'Ufficio ha ricordato che, in considerazione dell'impossibilità di identificare con certezza tutti i pazienti con infezione da HIV, il legislatore ha previsto alcune precauzioni finalizzate alla protezione dal contagio nei confronti della generalità delle persone assistite. A seguito dell'intervento dell'Ufficio, il dentista ha comunicato di aver adeguato la scheda anamnestica utilizzata nel proprio studio alle prescrizioni contenute nel citato provvedimento del 2009 (note 6 febbraio e 2 aprile 2013).

5.2. *Il trattamento di dati sanitari per fini amministrativi*

Numerosi sono stati gli interventi con riferimento ai trattamenti di dati idonei a rivelare lo stato di salute effettuati da strutture sanitarie pubbliche per finalità amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale (Ssn) (art. 85, comma 1, lett. *a*), del Codice).

A seguito di numerose segnalazioni, il Garante ha adottato un provvedimento generale in merito al trattamento dei dati sanitari effettuato nella redazione delle certificazioni sull'invalidità civile. Il provvedimento si è reso necessario in quanto il decreto-legge in materia di semplificazioni del 2012 (d.l. 9 febbraio 2012, n. 5, convertito in legge, con modificazioni, 4 aprile 2012, n. 35) ha previsto che le attestazioni medico-legali richieste per il rilascio del contrassegno invalidi nonché per le agevolazioni fiscali relative ai veicoli per le persone con disabilità possano essere sostituite dal verbale della commissione medica integrata. Al riguardo, numerosi cittadini hanno lamentato la presenza nei suddetti verbali di informazioni sanitarie, quali dati anamnestici e diagnosi del soggetto sottoposto a controllo, non pertinenti né indispensabili ai fini dell'erogazione dei predetti benefici e che, quindi, non dovrebbero essere conoscibili da parte dei soggetti a ciò deputati. Il Garante, nel riconoscere la semplificazione che la norma richiamata intendeva introdurre, ha ritenuto che, al fine di dare attuazione ai princìpi di pertinenza, non eccedenza e indispensabilità, le commissioni mediche debbano rilasciare una copia del verbale della commissione medica priva delle parti dedicate alla descrizione dei dati anamnestici, all'esame obiettivo e alla diagnosi della persona con disabilità. Ciò affinché sia assicurato un elevato livello di tutela dei diritti e delle libertà, pur nel rispetto del principio di semplificazione (art. 2, comma 2, del Codice) (provv. 16 luglio 2013, n. 331, doc. web n. 2536504).

In un altro caso l'Autorità ha condiviso l'interpretazione prospettata dal Ministero delle infrastrutture e trasporti della disciplina in materia di rilascio delle patenti nautiche con riferimento alla documentazione di idoneità che deve essere presentata agli uffici amministrativi, con particolare riferimento al certificato di idoneità rilasciato dal medico legale. Al riguardo, il Ministero, ritenendo che la "dichiarazione sostitutiva del certificato anamnestico", contenente dati sanitari, debba essere custodita solo dal

medico legale che effettua la visita di idoneità e non debba essere allegata al certificato da presentare agli uffici amministrativi, ha assicurato che provvederà ad impartire (unitamente al Comando generale del Corpo delle Capitanerie di porto) istruzioni agli uffici deputati al rilascio delle patenti nautiche (nota 10 luglio 2013).

Nel corso del 2013 si sono resi necessari alcuni interventi del Garante anche con riferimento alle attività di controllo svolte dalle Aziende sanitarie in merito alle prestazioni erogate dalle strutture sanitarie convenzionate o accreditate con il Ssn. In un caso, l'Ufficio ha ritenuto conforme alla disciplina vigente e alla versione aggiornata dello schema tipo aggiornato di regolamento per il trattamento dei dati sensibili e giudiziari da parte delle Aziende sanitarie la richiesta avanzata dal nucleo operativo di controllo di una Asl nei confronti di un laboratorio di analisi convenzionato con il Ssn, volta ad ottenere la copia dei referti relativi ad alcune prestazioni erogate in determinati giorni. L'acquisizione di tali referti si era resa indispensabile per consentire all'azienda di effettuare una verifica approfondita sulla congruenza della prestazione erogata rispetto alle competenze corrisposte dalla Asl in relazione a specifici casi (nota 25 marzo 2013).

Trattamenti sanitari che prevedono l'utilizzo di cellule e tessuti umani per trapianti sperimentali

È stato reso un parere sullo schema di accordo tra il Governo, le Regioni e le Province autonome di Trento e di Bolzano sulle linee guida per la ricognizione dei trattamenti sanitari che prevedono l'utilizzo di cellule e tessuti umani per trapianti sperimentali e per medicinali per terapie avanzate al fine di rendere disponibili al Ministero della salute informazioni utili a valutare le reali potenzialità di impiego di tali trattamenti (parere 21 marzo 2013, n. 141, doc. web n. 2380087). In particolare, in attesa dell'istituzione di un registro nazionale (cfr. art. 12, d.l. 18 febbraio 2012, n. 179 convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221), lo schema prevede di raccogliere, per ciascuna tipologia di trattamento sanitario, dati relativi al numero dei pazienti coinvolti, alle patologie curate, alle tipologie di tessuti e di cellule utilizzati, nonché al numero delle reazioni o eventi avversi gravi.

Nel rendere il proprio parere, l'Autorità ha chiesto di introdurre opportuni accorgimenti di aggregazione delle informazioni da raccogliere al fine di escludere il rischio di identificazione, anche indiretta, dei pazienti interessati facendo riferimento ai parametri individuati dal codice deontologico per i trattamenti di dati personali per scopi statistici e scientifici (All. A. 4 al Codice).

6 I dati genetici

Con specifico riferimento alle ricerche scientifiche in campo medico biomedico ed epidemiologico effettuate mediante l'utilizzo di dati genetici e di campioni biologici raccolti a fini di tutela della salute, l'autorizzazione generale – adottata con provv. 13 dicembre 2012 (doc. web n. 2157564), sentito il Ministro della salute, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità – consente, in casi residuali, di procedere al trattamento dei dati anche in assenza del consenso degli interessati. Ciò quando, a causa di particolari ragioni, non è possibile informare gli interessati malgrado sia stato compiuto ogni ragionevole sforzo per raggiungerli e a condizione che sia acquisito il parere favorevole del competente comitato etico a livello territoriale e sia rilasciata un'apposita autorizzazione dal Garante ai sensi dell'art. 90 del Codice.

Al riguardo, nel rispondere ad una società farmaceutica che aveva richiesto all'Autorità un'autorizzazione *ad hoc* per il trattamento di dati genetici, in assenza del consenso degli interessati, al fine di eseguire uno studio non interventistico retrospettivo sui tumori gastrointestinali, l'Ufficio, nel raccomandare di verificare in via preliminare se le informazioni che si prevedeva di raccogliere per la conduzione dello studio rientrassero effettivamente tra i "dati genetici", tenuto conto della definizione contenuta nella citata autorizzazione generale, ha precisato che tra queste informazioni rientrano anche quelle riguardanti mutazioni rilevabili sul tessuto tumorale che possono essere presenti anche nella linea germinale e quindi trasmissibili per via ereditaria (v. punto 1. *a*), Aut. gen. n. 8 cit.) (nota 19 luglio 2013).

Sempre con riferimento a ricerche scientifiche effettuate con dati e campioni raccolti in precedenza a fini di tutela della salute, il Garante ha rilasciato ad un'azienda ospedaliero-universitaria un'autorizzazione ai sensi dell'art. 90 del Codice (provv. 20 giugno 2013, n. 306, doc. web n. 2553271 e 30 gennaio 2014, n. 51, doc. web n. 2939000). L'azienda in questione aveva richiesto all'Autorità di poter trattare, anche in assenza del consenso di tutti i pazienti coinvolti, dati sanitari e genetici di circa duecento persone per la conduzione di uno studio finalizzato a monitorare gli esiti clinici (quali la morte, la sopravvivenza, lo sviluppo di complicanze, *etc.*) di malati con cirrosi epatica sottoposti a trapianto di fegato negli anni 2005-2010 presso la medesima azienda – compresi i pazienti deceduti nel periodo successivo al trapianto. La richiesta di autorizzazione era motivata dalla necessità di evitare distorsioni nei risultati dello studio derivanti dalle modalità di selezione della popolazione inclusa, considerata la significatività della sopravvivenza del paziente – quale esito clinico del trapianto – e l'incidenza della mortalità nei pazienti affetti da cirrosi epatica.

Lo studio aveva ricevuto anche il motivato parere favorevole del competente comitato etico a livello territoriale. Esso prevedeva, in particolare, che i dati genetici dei pazienti fossero ricavati dall'analisi di campioni di tessuto epatico prelevati sia dal fegato espiantato sia da quello impiantato; che i campioni biologici prelevati fossero distrutti al termine della ricerca e che i dati raccolti fossero conservati per un periodo di tempo non superiore a dieci anni e trasformati in seguito in forma anonima. I campioni di tessuto epatico prelevati sarebbero stati, inoltre, utilizzati soltanto dall'azienda e trasmessi ad un centro di ricerca biomedica per l'analisi genetica.

Nell'accogliere la richiesta, il Garante, rilevato che lo studio prevedeva la partecipazione su base volontaria dei pazienti risultanti in vita (con l'acquisizione del relativo

consenso al trattamento dei dati), ha disposto che il trattamento poteva essere effettuato, anche in assenza del consenso, limitatamente ai pazienti deceduti che non si fossero opposti in vita all'uso dei loro dati e campioni a scopo di ricerca. Ha richiesto, inoltre, all'azienda di riformulare il modulo dell'informativa (da sottoporre ai pazienti in vita) precisando l'ambito di comunicazione dei dati e di designare il centro di ricerca biomedica che collaborava alla realizzazione dello studio come responsabile del trattamento. È stato prescritto infine all'azienda di adottare idonee misure di sicurezza con specifico riferimento all'uso di sistemi di autenticazione basati anche su dispositivi biometrici per la consultazione dei dati genetici con strumenti elettronici, nonché di locali protetti per il trattamento dei campioni biologici e di contenitori muniti di serratura o di dispositivi equipollenti per il trasporto degli stessi (v. in particolare, punto 4.3 aut. cit.). Ciò fermo restando che l'azienda avrebbe potuto utilizzare i soli dati strettamente indispensabili e pertinenti per la conduzione dello studio.

Si segnala infine che, a fine 2013, l'autorizzazione generale sui dati genetici è stata rinnovata per un altro anno, in termini sostanzialmente analoghi alla precedente (provv. 12 dicembre 2013, n. 571, doc. web n. 2818993).

7 La ricerca scientifica e la statistica

7.1. *La ricerca scientifica*

Anche nel 2013, l'Ufficio ha comunicato, in diverse occasioni, a enti di ricerca, società scientifiche ed università che, sulla base dell'autorizzazione generale n. 9 al trattamento dei dati personali effettuato per eseguire studi e ricerche in campo medico, biomedico e epidemiologico, nel caso in cui risulti impossibile rendere l'informativa agli interessati, non è più necessario ottenere, caso per caso, specifiche autorizzazioni da parte dell'Autorità (nota 17 luglio 2013).

Tale autorizzazione, rinnovata per tutto il 2014 in termini sostanzialmente analoghi alla precedente (provv. 12 dicembre 2013, n. 572, doc. web n. 2818670), prende in considerazione, infatti, le ragioni più ricorrenti poste a fondamento dell'impossibilità di fornire l'informativa agli interessati nella conduzione di studi, non aventi significativa ricaduta personalizzata sugli interessati, effettuati con dati sanitari (oppure sulla vita sessuale e sull'origine razziale ed etnica) raccolti in precedenza a fini di cura della salute o per l'esecuzione di precedenti progetti di ricerca ovvero ricavati da campioni biologici prelevati in precedenza per le stesse finalità. In particolare, ove necessario per la ricerca, l'utilizzo delle predette informazioni è consentito, anche in assenza del consenso dei pazienti interessati, qualora non sia possibile informarli sul trattamento dei loro dati per "motivi etici" o "motivi di impossibilità organizzativa" e a condizione che sul progetto di ricerca si sia espresso favorevolmente, con parere motivato, il comitato etico territorialmente competente (artt. 107 e 110 del Codice). È invece obbligatorio acquisire il consenso degli interessati quando questi risultino reperibili e, in particolare, quando si rivolgano nuovamente al centro di cura, anche per visite di controllo. È inoltre necessaria una specifica autorizzazione del Garante per circostanze del tutto particolari o situazioni eccezionali non considerate nell'autorizzazione generale.

Con riferimento ai trattamenti effettuati per scopi statistici o scientifici rispetto a dati originariamente raccolti per altri scopi, l'Autorità si è occupata delle modalità alternative per rendere l'informativa agli interessati, quando questa richieda uno sforzo sproporzionato rispetto al diritto tutelato e siano adottate idonee forme di pubblicità, individuate dal pertinente codice deontologico (artt. 105, comma 4, del Codice e 6, commi 4 e 5, del codice deontologico per i trattamenti di dati personali per scopi statistici e scientifici).

Un caso esaminato dal Garante ha riguardato un progetto di ricerca – promosso dall'Agenzia per i servizi sanitari regionali (Age.na.s) in collaborazione con un'Agenzia regionale di sanità (Ars) e un istituto di ricerca del Cnr – finalizzato a costruire e a verificare nuovi algoritmi per individuare i casi di pazienti affetti da patologie complesse o croniche. In particolare, il progetto – incluso nel programma nazionale per la ricerca sanitaria di cui all'art. 12-*bis*, d.lgs. n. 502/1992 – prevedeva, in una prima fase, di selezionare dagli archivi amministrativi informatizzati delle Asl un campione di circa 50.000 assistiti affetti da patologie complesse o croniche utilizzando alcuni algoritmi e, in una seconda fase, di verificare la validità di questi ultimi confrontando i risultati così ottenuti con i dati sanitari riferiti a ciascuno degli assistiti inclusi nel campione ed estrapolati dai *database* clinici dei medici di medicina gene-

rale (mmg). Avuto riguardo all'elevato numero di soggetti interessati e alla loro distribuzione sul territorio, l'Age.na.s aveva giudicato sproporzionato informare singolarmente i pazienti coinvolti.

In questa cornice l'Autorità, nell'accogliere la richiesta, ha ritenuto che fosse possibile assolvere l'obbligo tramite le forme alternative di pubblicità prospettate dall'Agenzia in conformità a quelle individuate nel codice deontologico per i trattamenti di dati personali per scopi statistici e scientifici (art. 6, comma 4). In particolare, l'Agenzia aveva previsto di rendere l'informativa tramite un'inserzione su un quotidiano di larga diffusione in ciascuno dei territori provinciali di riferimento e, quale ulteriore forma di pubblicità, in considerazione delle peculiarità del progetto di ricerca, di riprodurre l'informativa anche su pieghevoli da affiggere e distribuire nelle sale di attesa delle Asl e degli studi dei mmg coinvolti.

Nondimeno, per garantire la più ampia conoscibilità dei trattamenti di dati effettuati nell'ambito della ricerca, l'Autorità ha fornito all'Age.na.s talune prescrizioni aggiuntive disponendo che l'informativa sui quotidiani individuati dall'Agenzia venisse pubblicata nelle giornate di maggiore distribuzione e che fosse divulgata anche tramite i siti istituzionali delle Asl interessate, in modo facilmente reperibile e visibile fino alla conclusione del progetto. Infine, è stato richiesto all'Agenzia di garantire che i medici di base coinvolti nella ricerca fossero in grado di illustrare in modo chiaro e completo, ai pazienti che ne avessero fatto richiesta, gli elementi essenziali del trattamento dei dati, predisponendo nei riguardi dei predetti professionisti, ove necessario, appositi interventi formativi (provv. 18 luglio 2013, n. 359, doc. web n. 2578223).

In un altro caso portato a conoscenza dell'Ufficio, ai sensi degli artt. 19, comma 2 e 39 del Codice, è stato precisato che la speciale disciplina prevista per le comunicazioni tra soggetti pubblici, in assenza di una specifica norma di legge o di regolamento, riguarda esclusivamente dati personali diversi da quelli sensibili. Il caso riguardava un'università che voleva realizzare un programma di sorveglianza sanitaria della popolazione residente in prossimità di un inceneritore per rifiuti solidi urbani, utilizzando dati personali raccolti presso l'Inps. Al riguardo, è stato rilevato che la comunicazione da parte dell'Inps dei dati nominativi delle lavoratrici occupate in aziende ricadenti su un'area del territorio esposto alle ricadute dei contaminanti dell'inceneritore poteva essere avviata soltanto nella misura in cui le informazioni oggetto di comunicazione non fossero idonee a rivelare lo stato salute delle interessate (come nel caso in cui l'insieme di queste informazioni possa palesare un rischio di malattia per le interessate).

Al riguardo, è stato altresì evidenziato che il trattamento dei dati nominativi e sanitari delle lavoratrici previsto dal programma di sorveglianza poteva essere effettuato dall'università soltanto in presenza di presupposti giuridici idonei a legittimarlo in conformità alle speciali disposizioni dettate dal codice in materia di ricerca scientifica (cfr. artt. 107 e ss. e codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici – Allegato A.4. del Codice).

Come è noto, in base alla predetta disciplina (art. 110 del Codice), la possibilità di trattare dati sulla salute per ricerche mediche, biomediche ed epidemiologiche è ammessa, a prescindere dal consenso delle persone interessate, quando il trattamento è previsto da una legge o rientra in un programma di ricerca biomedica o sanitaria di cui all'art. 12-*bis*, d.lgs. n. 502/1992 e ne sia stata data preventiva comunicazione al Garante (art. 39, comma 1, lett. *b*), del Codice). È consentito inoltre prescindere dal consenso degli interessati nell'ipotesi in cui non sia possibile, a causa di particolari ragioni, rendere loro l'informativa e il programma di ricerca sia oggetto di parere favorevole del competente comitato etico e sia, altresì, autorizzato dal Garante (nota 31 dicembre 2013).

In tema di ricerca scientifica, merita accennare anche al caso di un'università che ha presentato un'istanza, ai sensi degli artt. 19, comma 2 e 39 del Codice, finalizzata a raccogliere presso le Corti d'appello circoscrizionali dati relativi alla residenza dei candidati alle scorse elezioni politiche al fine di realizzare un progetto, finanziato dal Miur, sul cambiamento della rappresentanza politica in Italia negli anni 2013-2015. Il progetto prevedeva che un campione di candidati fosse intervistato con questionari inviati a mezzo posta. Con riferimento ai soggetti per i quali non fosse stato possibile acquisire le residenze presso le Corti d'appello, l'università intendeva acquisire l'informazione relativa al domicilio fiscale dei candidati presso l'Agenzia delle entrate. L'università garantiva, inoltre, che l'indagine sarebbe stata svolta nel pieno rispetto del Codice e del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, Allegato A.4. al Codice. Su tali basi, l'Ufficio, rilevata nel caso di specie la necessità dei dati in questione per lo svolgimento delle funzioni istituzionali dell'università, ha ritenuto di non dover formulare alcuna osservazione, tenuto conto che il Codice dispone, sia pure come ipotesi residuale, che in mancanza di una specifica norma di legge o di regolamento che lo preveda, le amministrazioni pubbliche possano comunicare ad altri soggetti pubblici dati personali, non aventi natura sensibile, allorquando tale trattamento sia necessario per lo svolgimento delle proprie funzioni istituzionali, previa comunicazione al Garante (artt. 18, comma, 2, 19, comma 2 e 39, del Codice) (nota 28 giugno 2013).

7.2. *La statistica*

Il Garante è intervenuto in relazione al trattamento di dati personali raccolti nell'ambito del 15° Censimento generale della popolazione e delle abitazioni rappresentando ad un segnalante che i dati anagrafici contenuti nella lista A dei questionari di famiglia e convivenza sono stati trattati, oltreché dall'Istat per finalità statistiche, anche da parte dei comuni per il perseguimento della finalirà amministrativa di revisione post-censuaria delle anagrafi. Tale circostanza, resa nota anche nella lettera informativa dell'Istat ai cittadini, è stata prevista, in particolare, dall'art. 50, comma 2, lett. *d*), d.l. 31 maggio 2010, n. 78, convertito con modificazioni, dall'art. 1, comma 1, l. 30 luglio 2010, n. 122, che ha affidato all'Istat la definizione delle "modalità per il confronto contestuale alle operazioni censuarie tra dati rilevati al censimento e dati contenuti nelle anagrafi della popolazione residente, nonché, d'intesa con il Ministero dell'interno, le modalità di aggiornamento e revisione delle anagrafi della popolazione residente sulla base delle risultanze censuarie" (nota 19 luglio 2013).

Nell'ambito di un'istruttoria relativa alle modalità di raccolta e alle conseguenze del mancato conferimento dei dati personali, anche di natura sensibile, nell'ambito di un'indagine statistica realizzata dall'Istat, l'Ufficio ha richiesto informazioni all'Istituto circa le garanzie individuate in concreto per la raccolta dei dati personali idonei a rivelare lo stato di salute nell'ambito della predetta indagine, con particolare riferimento alle modalità con le quali si è inteso assicurare in concreto il diritto degli interessati a non rispondere a "quesiti di natura sensibile". Infatti, da una preliminare analisi dei pertinenti modelli di rilevazione presenti sul sito istituzionale dell'Istat (sia quelli da compilarsi a cura dell'intervistatore, sia quelli di autocompilazione), diversamente da quanto previsto per altre rilevazioni (ad es., il modello utilizzato per il censimento), è emerso che non veniva specificata – in relazione ai singoli quesiti o gruppi di quesiti – la natura degli stessi (riferito a dati sensibili o meno), né la facoltatività della risposta, rendendo così poco agevole per l'interessato la comprensione dei casi in cui non vi è obbligo di risposta e, quindi, delle conseguenze di un eventuale rifiuto a rispondere.

L'Istat ha evidenziato che tale rilevazione viene affidata ad intervistatori appositamente formati e istruiti per interagire direttamente con gli interessati, informandoli oralmente e segnalando puntualmente i quesiti ai quali è obbligatorio rispondere e quelli per i quali è facoltativo in ragione della presenza di dati sensibili nella risposta. In seguito alla richiesta dell'Autorità, l'Istituto ha deciso di integrare anche il testo dell'informativa scritta indicando l'elenco dei quesiti che comportano il trattamento di dati sensibili (per i quali, quindi, non vi è obbligo di risposta per gli interessati) (nota 20 febbraio 2013).

L'Autorità si è occupata anche della fornitura da parte del Ministero della salute di microdati derivanti dal Sistema informativo nazionale per le dipendenze (Sind) alla Presidenza del Consiglio dei Ministri per alimentare l'Osservatorio permanente istituito presso il Dipartimento politiche antidroga al fine di garantire che tali dati, come previsto dal quadro normativo vigente, risultino privi di ogni riferimento che ne permetta il collegamento con gli interessati e comunque secondo modalità che rendano questi ultimi non identificabili. Il flusso di dati Sind volto ad alimentare periodicamente e sistematicamente l'Osservatorio può, pertanto, avere ad oggetto anche microdati individuali relativi al fenomeno della tossicodipendenza, purché questi siano anonimi. Compete quindi al Ministero, titolare del trattamento dei dati personali (anche sensibili) contenuti nel Sind, e al Dipartimento assicurare, ciascuno in relazione alle proprie competenze, con idonee misure e accorgimenti, che i dati registrati presso l'Osservatorio, in origine o a seguito di trattamento, non possano essere associati a interessati identificati o identificabili (art. 4, comma 1, lett. *n*), del Codice).

In seguito all'istruttoria, che ha coinvolto anche le competenti strutture dell'Istat, il Ministero della salute ha comunicato al Garante di aver individuato una soluzione per effettuare la predetta fornitura nel rispetto del Codice, valutando il rischio di identificazione degli interessati censiti nella banca dati Sind sulla base del codice di deontologia e di buona condotta per i trattamenti di dati personali per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (allegato A.3. al Codice) (note 6 marzo e 28 giugno 2013).

8 I trattamenti da parte di Forze di polizia e per finalità di *intelligence*

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

A seguito di segnalazioni ricevute, l'Autorità ha continuato ad assicurare 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. *Gli altri interventi in relazione alle Forze di polizia*

Affissione e trasmissione dal Ministero della giustizia alle OO.SS. dell'elenco nominativo degli agenti di polizia penitenziaria che effettuano lavoro straordinario

Un agente del Corpo della polizia penitenziaria ha segnalato l'affissione mensile, in alcuni locali del Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia, dell'elenco del personale del Corpo nei confronti del quale era stata disposta la liquidazione del compenso per prestazioni di lavoro straordinario, con l'indicazione del numero di ore effettuate e di quelle retribuite o compensate con turni di riposo, nonché la trasmissione di tale elenco alle organizzazioni sindacali.

A tale proposito, richiamati i principi di necessità, non eccedenza, liceità e qualità dei dati (artt. 3 e 11 del Codice) nonché le disposizioni specifiche dettate per il trattamento dei dati da parte dei soggetti pubblici (nella specie, in particolare, gli artt. 18 e 19, comma 3 del Codice), il Garante ha osservato che le "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", adottate il 14 giugno 2007 (in G.U. 13 luglio 2007, n. 161, doc. web n. 1417809), prevedono, che non è di regola lecito per il datore di lavoro pubblico diffondere informazioni personali riferite a singoli lavoratori (punto 6.3) e che, in difetto di disposizioni del contratto collettivo applicabile che prevedano espressamente che l'informazione sindacale abbia ad oggetto anche dati nominativi del personale, l'amministrazione può fornire alle organizzazioni sindacali solo dati numerici o aggregati (punto 5).

Nella specie, il Garante, rilevata la mancanza di specifica fonte normativa o negoziale (non rinvenibile, in particolare, nell'art. 10, comma 9, dell'Accordo nazionale quadro per il personale appartenente al Corpo di polizia penitenziaria) che preveda che gli elenchi relativi al personale che effettua lavoro straordinario, oggetto di affissione e comunicazione alle organizzazioni sindacali, venga redatto con l'indicazione del nominativo dei lavoratori interessati, ha dichiarato illecito il relativo trattamento, vietandone la prosecuzione da parte del Dipartimento dell'amministrazione penitenziaria, che ha ottemperato (provv. 18 luglio 2013, n. 358, doc. web n. 2578201).

Ostensione da parte degli ospedali alla polizia amministrativa della certificazione medica relativa a persone coinvolte in sinistri stradali

Una Prefettura ha sottoposto un quesito relativo alla legittimità del diniego, da parte di un ospedale, all'ostensione agli organi di polizia amministrativa della certificazione medica relativa a persone coinvolte in sinistri stradali, ai fini della successiva trasmissione alla prefettura per la determinazione del periodo di sospensione della patente di guida del conducente responsabile del sinistro, *ex* artt. 222 e ss. del codice della strada. Ritenuto che la comunicazione tra pp.aa. di dati sensibili per finalità

amministrative è ammessa dal Codice unicamente quando è prevista da una norma di legge o di regolamento (art. 19, comma 3), l'Ufficio ha chiarito che il trattamento in oggetto può essere legittimamente effettuato dalle Aziende sanitarie solo ove sia previsto nel relativo regolamento adottato in conformità allo schema tipo sul quale il Garante ha espresso parere favorevole con provvedimento del 26 luglio 2012, n. 220 (doc. web n. 1915390). Laddove si renda, tuttavia, indispensabile trattare ulteriori categorie di dati, o eseguire altre operazioni di trattamento per perseguire finalità di rilevante interesse pubblico individuate dalla legge, le integrazioni o modifiche devono essere sottoposte al parere del Garante (nota 12 aprile 2013).

Conferenze stampa nel corso di indagini giudiziarie

Un avvocato, in qualità di difensore d'ufficio di una persona indagata in un procedimento penale, ha lamentato una violazione della disciplina in materia di protezione dei dati personali da parte di funzionari di polizia che nel corso di una conferenza stampa avevano divulgato, oltre alla forografia e alle generalità del suo assistito, anche presunte frasi a lui attribuite e particolari del crimine che avrebbero potuto rilevarsi, per la natura del reato e il coinvolgimento dei familiari della persona offesa, pericolosi per l'incolumità dell'indagato e forieri di problemi di ordine pubblico.

L'Ufficio ha evidenziato che, come emerso nel corso dell'istruttoria, obiettivo della conferenza stampa era accertare se l'interessato si fosse reso protagonista di episodi simili ai danni di altre persone. La diffusione delle informazioni a livello locale e la loro conoscenza da parte della collettività avrebbe potuto rivelarsi utile, se non necessaria, per verificare se altre persone avessero subito i medesimi abusi. In tale situazione, pur considerando le ragioni di riservatezza e di presunta incolumità dell'interessato, doveva ritenersi lecita, ai sensi degli artt. 11 e 47 del Codice, la divulgazione – peraltro autorizzata dalla Procura della Repubblica competente – dei dati dell'indagato e delle circostanze della vicenda, tenuto conto delle esigenze di giustizia sottese alla diffusione delle informazioni (nota 25 gennaio 2013).

Accertamenti di polizia giudiziaria

Sono stati chiesti chiarimenti da parte di un medico, amministratore unico e legale rappresentante di uno studio medico, riguardo alle informazioni che, senza ledere la riservatezza dei pazienti, è possibile comunicare su richiesta della polizia giudiziaria (nella specie, se una determinata persona si fosse recata presso il suo studio medico, quali esami avesse svolto e se in regime di convenzione o mediante pagamento da parte dell'assistito).

Al riguardo l'Ufficio ha evidenziato che, ai sensi dell'art. 256 c.p.p., i medici – al pari degli altri soggetti indicati negli artt. 200 e 201 c.p.p. – devono consegnare all'autorità giudiziaria che ne faccia richiesta, tra l'altro, gli atti, i documenti e le informazioni di cui siano in possesso per ragioni della loro professione, salvo che dichiarino per iscritto che si tratta di segreto inerente alla loro professione. Peraltro, l'autorità giudiziaria che ritiene di non potere procedere senza acquisire gli atti può provvedere alla verifica di tale dichiarazione e, se risulta infondata, può disporne il sequestro. Risulta quindi necessario che il medico verifichi se i dati oggetto della richiesta della polizia giudiziaria rientrino tra quelli coperti dal segreto professionale, attenendosi, in tal caso, a quanto prevede l'art. 256 c.p.p. (nota 16 aprile 2013).

Accesso delle OO.SS. negli istituti penitenziari

L'Autorità ha fornito riscontro a un quesito del Dipartimento dell'amministrazione penitenziaria del Ministero della giustizia concernente la possibilità da parte delle organizzazioni sindacali di effettuare riprese foto-video nel corso delle visite sui luoghi di lavoro degli istituti penitenziari previste dall'art. 5, comma 6, dell'Accordo nazionale quadro del 24 marzo 2004, il quale afferma che la visita dei rappresentanti sindacali "è diretta a verificare esclusivamente le condizioni logistiche dei vari luoghi di lavoro".

L'Ufficio ha rilevato che la disposizione risulta fare chiaro riferimento alla verifica dei luoghi frequentati dagli agenti della polizia penitenziaria nello svolgimento della loro attività lavorativa – quali uffici, spazi dedicati alla custodia dei detenuti, locali

vari, eventuali apparecchiature utilizzate, postazioni di lavoro, *etc.* – in funzione della loro idoneità a consentire l'espletamento dei compiti di istituto in condizioni di salubrità e sicurezza. In tale contesto, le ipotizzare riprese foto-video vanno limitate alle sole condizioni degli ambienti, con esclusione di profili attinenti alla protezione dei dati personali. L'eventuale coinvolgimento nelle riprese del personale operante negli istituti, come pure dei detenuti ivi ristretti, in quanto non essenziale rispetto al fine del controllo dei luoghi di lavoro demandato alle organizzazioni sindacali dal contratto collettivo, comporterebbe, infatti, un trattamento di dati effettuato in violazione del principio di necessità ed eccedente rispetto alle finalità perseguite con le verifiche previste dalla contrattazione (cfr. artt. 3 e 11, comma 1, lett. *d*), del Codice) (nota 10 maggio 2013).

8.2.1. I sistemi di videosorveglianza per finalità di pubblica sicurezza

Visione degli interni di private abitazioni da parte di telecamere installate per motivi di pubblica sicurezza

L'Autorità ha ricevuto la segnalazione di alcuni cittadini, residenti in diversi comuni, circa la presenza di telecamere di videosorveglianza che, pur installate sulla pubblica via, consentivano, a causa della loro ubicazione, una visione diretta anche degli interni delle abitazioni dei segnalanti. Gli accertamenti effettuati dall'Autorità hanno permesso di appurare che le telecamere erano state installate in attuazione del "Programma Operativo Nazionale (PON) – Sicurezza per lo Sviluppo – Obiettivo convergenza 2007-2013", gestito dal Ministero dell'interno, e che la titolarità del trattamento dei dati era stata conferita alla locale questura. Il Garante ha ritenuto che, ancorché gli obiettivi del menzionato programma – riconducibili alla prevenzione e al contrasto alla criminalità – apparissero condivisibili e di notevole rilevanza sociale, i trattamenti di dati personali effettuati tramite l'utilizzo di sistemi di videosorveglianza, quand'anche riconducibili a quelli previsti dall'art. 53 del Codice, debbono rispettare i principi posti dall'art. 11 del Codice medesimo e, in particolare, il principio secondo il quale i dati personali oggetto di trattamento debbono essere pertinenti e non eccedenti rispetto alle finalità per le quali i dati sono raccolti o successivamente trattati, come ribadito dal Garante anche nel provvedimento generale in materia di videosorveglianza adottato l'8 aprile 2010 (doc. web n. 1712680). La possibilità per le telecamere in argomento di effettuare riprese anche all'interno degli immobili dei segnalanti configura quindi un trattamento di dati personali illecito in quanto eccedente e non pertinente rispetto alle finalità di prevenzione e contrasto alla criminalità per le quali i dati sono raccolti. Pertanto, il Garante ha vietato alla questura il trattamento dei dati personali dei segnalanti attraverso le citate telecamere di sorveglianza, prescrivendo, altresì, di adottare ogni misura necessaria atta a impedire la possibilità di effettuate riprese dell'interno delle abitazioni dei medesimi, dandone riscontro al Garante. Il titolare del trattamento ha provveduto ad apportare al sistema di videosorveglianza le modifiche richieste (provv.ti 27 giugno 2013, n. 316, doc. web n. 2576958 e n. 317, doc. web n. 2577003).

Tempi di conservazione delle immagini riprese dai sistemi di videosorveglianza della polizia municipale

Il Corpo della polizia municipale di un Comune ha chiesto se, per corrispondere alle eventuali esigenze investigative delle Forze di polizia, era possibile prolungare fino ad un periodo di 60 giorni i tempi di conservazione delle immagini delle targhe di veicoli registrate dal sistema di videosorveglianza gestito dal Corpo medesimo. L'Ufficio ha rilevato che il paragrafo 3.4. del provvedimento generale in materia di videosorveglianza, prevede che i comuni, in caso di videosorveglianza finalizzata alla tutela della sicurezza urbana, possono conservare i dati nel termine massimo di sette giorni successivi alla rilevazione delle immagini e che, in caso di effettive ed eccezionali esigenze di ulteriore conservazione, devono inoltrare al Garante una richiesta di verifica preliminare, adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti

eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità.

Con riferimento al caso di specie, il provvedimento consente quindi un prolungamento del termine di conservazione delle immagini anche in presenza di richieste della polizia giudiziaria motivate però in relazione a specifiche e puntuali attività investigative in corso, dovendosi escludere una preventiva e generalizzata conservazione ultrasettimanale per esigenze solo eventuali (nota 9 dicembre 2013).

Videosorveglianza all'interno delle camere di sicurezza

Un Comune ha posto un quesito relativo alla liceità del trattamento dei dati personali svolto per mezzo dell'installazione di telecamere che riprendano l'interno delle camere di sicurezza del comando della polizia municipale ove, ai sensi degli artt. 380 o 381 c.p.p., vengono rinchiusi gli arrestati in flagranza di reato da personale con qualifica di agente od ufficiale di polizia giudiziaria. Il Comune ha evidenziato che le immagini sarebbero state visionate dal personale del comando e conservate per un massimo di 24 ore, consentendo di poter controllare a distanza i detenuti al fine di intervenire in caso di tentativo di evasione e per evitare possibili atti di autolesionismo.

Fornendo riscontro, l'Aurorità ha rappresentato che la circostanza che le camere di sicurezza debbano essere sottoposte a sorveglianza non implica per ciò solo che sia previsra e consentita l'installazione di telecamere che riprendano l'interno delle stesse. Rilevato che non risulta sussistere – né è stata indicata dal comando – alcuna specifica normativa concernente la videosorveglianza nelle camere di sicurezza, è stato evidenziato che la Corte di cassazione, nel pronunciarsi su una vicenda relativa ad un detenuto sottoposto al regime di cui all'art. 41-*bis*, l. n. 354/1975, ha ritenuto illegittimo il ricorso alla videosorveglianza totale dello stesso – anche nel momento dell'utilizzo della *toilette* –, valutando idonei a prevenire possibili aggressioni alla persona del detenuto i controlli fisici diretti mediante feritoie ed oblò (Cass. pen., sez. V, 26 aprile 2011). Occorre dunque assumere come riferimento la normativa generale in materia di protezione dei dati posta dal Codice e, più specificamente, i principi posti dall'art. 11, oltre alle prescrizioni contenute nel provvedimento generale del Garante in materia di videosorveglianza.

In particolare, nella materia rilevano i principi di necessità e di proporzionalità nel trattamento dei dati, rispetto ai quali occorre valutare, ad esempio, se sia necessario installare le telecamere all'interno delle camere di sicurezza o se sia sufficiente posizionarle negli ambienti attigui alle celle, oppure ancora se corrisponda alle esigenze esposte dal comando dotare di telecamere solo una o più celle, da utilizzare nei soli casi, da valutare rigorosamente volta per volta, in cui sussistano effettive e concrete esigenze di prevenire possibilità di evasione o pericoli alla persona, rimanendo sempre ferma, come ha chiarito la citata pronuncia della Suprema Corte, la salvaguardia degli aspetti più intimi della sfera di riservatezza dell'interessato. Le conseguenti valutazioni non possono comunque essere assunte con carattere di generalità, ma devono essere svolte caso per caso e, ove ritenuto necessario il trattamento in esame, devono essere supportate da una circostanziata motivazione (nota 5 settembre 2013).

8.3. *Il controllo sul sistema di informazione Schengen*

Il Ministero dell'interno-Dipartimento della pubblica sicurezza ha rappresentato l'opportunità di differire l'adempimento delle ultime misure prescritte dal Garante volte a rafforzare la sicurezza nel trattamento dei dati effettuati per l'attuazione della Convenzione di Schengen, in ragione sia delle innovazioni tecnologiche introdotte con l'entrata in funzione del nuovo Sistema di informazione Schengen (SIS II), sia

delle difficoltà di realizzazione dei progetti, legate soprattutto alla disponibilità delle necessarie risorse finanziarie.

Alla luce delle indicazioni ricevute e delle difficoltà rappresentate dal Ministero, il Garante con provvedimenti del 24 gennaio 2013, n. 23 (doc. web n. 2324763) e 1° agosto 2013, n. 379 (doc. web n. 2635313) ha disposto il differimento dei termini per l'adempimento delle prescrizioni, che sono in corso di attuazione.

Accesso diretto

Il Codice ha introdotto nuove modalità di esercizio dei diritti relativamente ai dati registrati nell'N-SIS, in virtù delle quali l'interessato può rivolgersi in Italia direttamente all'autorità che ha la competenza centrale per la sezione nazionale del SIS, ossia al Dipartimento della pubblica sicurezza (cd. accesso diretto). Il numero e il contenuto delle richieste degli interessati che ancora pervengono direttamente al Garante sono rimaste stabili rispetto all'anno precedente.

Hanno invece subito un lieve aumento le richieste di accesso ai dati pervenute al Garante da Autorità di controllo di sezioni nazionali del SIS di altri Stati, interpellate dagli interessati in relazione a segnalazioni inserite nel sistema da autorità di polizia italiane. Le informazioni sono state comunicate, previa consultazione degli uffici segnalanti, nel rispetto delle disposizioni degli artt. 109 e 114 della Convenzione.

8.4. *Il* Datagate *e i trattamenti per finalità di* intelligence

A fronte delle notizie, riportate dalla stampa, sul cd. *Datagate* – ovvero sulla raccolta di dati personali di milioni di cittadini, non solo statunitensi, da parte della *National Security Agency* (NSA) – il Garante ha svolto una serie di attività informative e di impulso nei confronti del Governo, al fine di minimizzare i rischi per i cittadini italiani rispetto ad eventuali acquisizioni dei loro dati per fini di *intelligence*.

In primo luogo, il 23 luglio 2013 il Garante è stato audito, ai sensi dell'art. 31, comma 3, l. n. 124/2007, dal Comitato parlamentare per la sicurezza della Repubblica (Copasir), in relazione alle implicazioni sui diritti dei cittadini europei alla raccolta di dati personali per fini di *intelligence* svolta in base al *Foreign Intelligence Surveillance Act* (FISA) e al rapporto tra protezione dati e trattamenti per fini di sicurezza dello Stato nel nostro ordinamento.

Il 22 ottobre, all'indomani dell'approvazione in Commissione LIBE del Parlamento europeo, della proposta di regolamento sulla protezione dei dati personali, il Garante, con una nota indirizzata al Presidente del Consiglio dei Ministri, ha segnalato l'esigenza di accertare se lo spionaggio anche telematico condotto dal NSA abbia coinvolto, sia pure incidentalmente, cittadini italiani, nonché la necessità di adottare efficaci strumenti di protezione dei dati personali trattati per fini di sicurezza, anche nella consapevolezza e condivisione dell'obiettivo europeo di rafforzare gli strumenti di cooperazione di polizia e giudiziaria (doc. web n. 2708275).

Infine, l'11 novembre 2013 il Garante e il Dipartimento delle informazioni per la sicurezza (Dis) della Presidenza del Consiglio dei Ministri hanno siglato un protocollo d'intenti volto a disciplinare alcune procedure informative funzionali all'esercizio delle rispettive attribuzioni. Il protocollo prevede, in particolare, modalità di informazione idonee a consentire al Garante di conoscere alcuni elementi essenziali del trattamento dei dati personali effettuato dagli Organismi per l'informazione e la sicurezza in alcuni contesti peculiari, segnatamente quelli concernenti la sicurezza cibernetica o gli accessi alle banche dati delle pp.aa. o degli esercenti servizi di pubblica utilità.

9 L'attività giornalistica

Tenendo conto delle diverse forme attraverso cui si esercita ormai la libertà di informazione, l'anno di riferimento è stato caratterizzato da un impegno costante nel valutare, nel quadro di riferimento del Codice (in particolare, artt. 136-139) e dell'allegato codice di deontologia, segnalazioni e reclami per lo più concernenti l'esercizio dell'attività giornalistica.

Accanto a tale attività, improntata al bilanciamento tra libertà di informazione e diritto alla riservatezza e alla protezione dei dati personali, è maturata la decisione di promuovere l'aggiornamento del codice di deontologia, adottato nel 1998, relativo al trattamento di dati personali in ambito giornalistico al fine di un suo adeguamento in considerazione dell'evoluzione tecnologica (che ha inciso su tecniche e modalità dell'informazione) e dell'evoluzione giurisprudenziale di alcuni istituti, quali il "diritto all'oblio" (cui peraltro fa riferimento la proposta di regolamento Ue in materia di protezione di dari personali).

Il Garante ha quindi deliberato l'avvio dei lavori, secondo la procedura di cooperazione con il Consiglio nazionale dell'Ordine dei giornalisti prevista dall'art. 139 del Codice, contemplando altresì la possibilirà di sentire, in rale ambito, anche soggetri rappresentativi dell'informazione *online* (provv. 1° agosto 2013, n. 376, in G.U. 23 agosto 2013, n. 197, doc. web n. 2564822). La presidenza dell'Ordine dei giornalisti e il Garante, renuto anche conto dei contributi pervenuti e degli elementi acquisiti dai soggetti interpellati, hanno lavorato ad una bozza di nuovo codice di deontologia da sottoporre al Consiglio dell'Ordine dei giornalisti nella riunione plenaria del 27-30 marzo 2014, nel corso della quale, tuttavia, il testo non è stato approvato.

Il Garante, nell'esprimere alla presidenza dell'Ordine il proprio rammarico per la valutazione negativa espressa dal Consiglio rispetto ad un lavoro attento e approfondito svolto anche con il proprio contributo, ha comunicato all'Ordine di non essere intenzionato ad esercitare i poteri sosritutivi offerti dall'art. 139 del Codice ai fini dell'approvazione del testo e di voler proseguire nei propri compiti attenendosi al codice di deontologia vigente.

9.1. *I minori*

Il delicato rapporto tra informazione e turela dei minori (nel quadro delle fonti sopra ricordate nonché della Carta di Treviso) conserva una posizione centrale nello svolgimento dei compiti istituzionali dell'Autorità. Nella vigente cornice normativa, come noto, il diritto del minore alla riservatezza deve sempre essere considerato prevalente rispetto al diritto di cronaca e, al fine di tutelarne la personalità, i giornalisti devono rendere non identificabili i minori coinvolti in fatti di cronaca (art. 7 codice di deontologia).

L'Autorità ha invocato tali principi nell'esaminare, in particolare, due casi, sottoposti alla sua attenzione da due Tribunali per i Minorenni, riguardanti delicate vicende familiari di affidamento. Nel primo caso una testata giornalistica locale aveva pubblicato la notizia del suicidio di una donna, madre di tre figli affidati a terzi (in ragione del problemarico contesto familiare in cui si trovavano) con un provvedimento giuri-

sdizionale; oltre alla foto e alle generalità della donna, il giornale aveva pubblicato quelle dei nonni e i nomi dei minori (questi ultimi contenuti nelle pagine del diario personale della madre, pure pubblicate dal quotidiano), rendendoli così direttamente identificabili (nota 22 febbraio 2013).

Nella seconda vicenda, un giornale locale aveva pubblicato il nome e il cognome di un minore, allontanato dai genitori con un provvedimento giurisdizionale, unitamente ad altre informazioni che ne evidenziavano la situazione di disagio e una possibile patologia; nell'articolo venivano altresì pubblicati i dati identificativi dell'intero nucleo familiare, compresi quelli dei fratelli, anch'essi minori (nota 13 settembre 2013).

L'Ufficio, nel ritenere entrambe le pubblicazioni contrastanti con la disciplina di protezione dei dati personali (oltre che con la Carta di Treviso che tutela espressamente "l'anonimato del minore per non incidere sull'armonico sviluppo della sua personalità"), ha ribadito che le garanzie a favore dei minori operano anche nell'eventualità che siano i genitori a rilasciare dichiarazioni alla stampa.

Analoghe valutazioni critiche sono state formulate in relazione alla perdurante diffusione, anche in rete, di notizie e immagini relative al bambino di Padova prelevato a scuola dalle Forze dell'ordine in esecuzione di un provvedimento giurisdizionale di affidamento, caso di cui l'Autorità si era già occupata (cfr. Relazione 2012, p. 148). Ulteriori segnalazioni concernenti la medesima vicenda hanno evidenziato che taluni organi di informazione, nel riferire dello svolgimento di un procedimento giudiziario coinvolgente i genitori, non solo hanno nuovamente fatto riferimento al minore – talvolta identificato nominativamente o, indirettamente, tramite i nominativi dei familiari – ma hanno anche riportato dichiarazioni rese dal padre nel corso del giudizio concernenti delicati episodi della vita privata del figlio. L'Ufficio ha considerato tale pubblicazione un'ulteriore significativa intrusione nella sfera privata del minore in violazione delle speciali garanzie dettate dall'ordinamento ed ha pertanto invitato gli editori interessati – che hanno formalmente aderito a tale richiesta – ad impegnarsi autonomamente a non diffondere ulteriormente, anche nelle edizioni *online* dei rispettivi giornali, dettagli relativi alla vita privata del minore (nota 5 dicembre 2013).

L'Autorità ha poi richiamato pubblicamente gli organi di informazione al rispetto del codice di deontologia e della Carta di Treviso in relazione alla diffusione di notizie concernenti fatti di cronaca di particolare risonanza avvenuti a Roma (una vicenda di prostituzione minorile e un tentativo di suicidio da parte di un sedicenne) rispetto ai quali sono stati via via diffusi – attraverso i *media* tradizionali e in rete – dettagli non essenziali lesivi della personalità e della dignità dei minori interessati, aumentando il rischio di una loro identificazione (comunicati stampa 29 maggio e 13 novembre 2013, docc. web nn. 2449404 e 2749736).

9.2. *La cronaca giudiziaria*

Notizie e immagini di arrestati e indagati

La materia della diffusione di informazioni relative a vicende giudiziarie ha continuato a formare oggetto di attenzione da parte dell'Autorità che ha ritenuto prive di fondamento segnalazioni nelle quali si lamentava la diffusione di dati identificativi di persone sottoposte ad indagine o condannate alla luce del principio, più volte ribadito nei suoi provvedimenti, secondo cui la pubblicazione di dati personali relativi a procedimenti penali è ammessa, anche senza il consenso dell'interessato, nei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico (art. 137, comma 3, del Codice; artt. 6 e 12 del codice di deontologia) (*ex pluribus*, note 15 marzo, 17 maggio e 21 ottobre 2013).

Pubblicazione di atti del procedimento e intercettazioni

Segnalazioni e reclami concernenti la cronaca giudiziaria talora hanno evidenziato profili di illiceità rispetto non solo al Codice, ma anche alle disposizioni in materia di segreto delle indagini e di pubblicazione degli atti processuali (artt. 114 e 329 c.p.p. e art. 684 c.p.).

In una vicenda, concernente la pubblicazione su un sito internet di un *e-book* recante il testo delle intercettazioni telefoniche raccolte nell'ambito di un'indagine coordinata dalla Procura della Repubblica di Napoli e contenute in un'informativa preliminare predisposta dai Carabinieri, anche alla luce del riscontro pervenuto dalla menzionata Procura, l'Autorità ha ritenuto che la pubblicazione, per le sue caratteristiche (il contenuto del libro coincideva con l'intero atto-informativa dei Carabinieri, comprensivo di intestazione, non sottoposto a rielaborazione alcuna), potesse presentare elementi di incompatibilità con l'art. 114, comma 2, c.p.p. – che vieta "la pubblicazione, anche parziale, degli atti non più coperti dal segreto fino a che non siano concluse le indagini preliminari ovvero fino al termine dell'udienza preliminare" –, sottoponendo quindi l'accertamento di tale circostanza alla competente autorità giudiziaria.

Si è d'altra parte evidenziato che, sotto il profilo delle specifiche disposizioni vigenti in materia di trattamento di dati personali in ambito giornalistico (artt. 136-139 del Codice), la pubblicazione, pur se attinente a fatti di indiscutibile interesse pubblico (risultanze di indagini su ipotesi di reato connessi alla gestione dei contributi pubblici erogati a favore di un movimento politico), contenesse alcune espressioni lesive della dignità della reclamante (senatrice, esponente del movimento interessato dalle indagini, menzionata nelle conversazioni intercettate), non rispondenti al parametro dell'"essenzialità dell'informazione", risultando la stessa di fatto estranea alla vicenda della gestione dei fondi pubblici attribuiti al movimento politico (nota 14 giugno 2013).

Vittime di reato

Particolare cautela nella diffusione di notizie relative a procedimenti penali deve essere adoperata a protezione del diritto alla riservatezza nonché per assicurare il rispetto della dignità delle persone offese dal reato, poiché la pubblicità (specie tramite internet) data alla lesione ne pregiudica ulteriormente i diritti. Questo orientamento è stato alla base della valutazione di illiceità della pubblicazione in rete, da parte di una testata locale, di due articoli (successivamente rimossi) nei quali erano stati riportati brani di un libro, incentrato sulla reclamante (peraltro con riferimenti lesivi della sua dignità) e sulla sua famiglia, dichiarato giudizialmente diffamatorio e oggetto di sequestro (nota 28 ottobre 2013).

9.3. *I personaggi pubblici*

Per quanto riguarda la diffusione di informazioni riguardanti personaggi pubblici o che esercitano pubbliche funzioni il quadro normativo e la relativa evoluzione giurisprudenziale consentono invece di individuare margini più ampi nel trattamento dei dati personali (in tal senso v. già Relazione 2012, p. 153).

Tale orientamento è stato seguito anche in relazione alla lamentata diffusione, nel corso di una trasmissione televisiva di inchiesta e di approfondimento informativo, di immagini tratte da un Dvd della festa nuziale privata dei segnalanti asseritamente sottratto agli stessi. Al riguardo, l'Ufficio ha rilevato che – fermi restando gli accertamenti dell'autorità giudiziaria in ordine all'asserita acquisizione fraudolenta del Dvd – la diffusione delle immagini ritraenti i segnalanti e alcuni ospiti (e tra questi un esponente politico già ministro dello sviluppo economico) non presentava profili di contrasto con il parametro della "essenzialità dell'informazione riguardo a fatti di interesse pubblico" (art. 137, comma 3, del Codice). Il servizio andato in onda – nel quale, peraltro, i volti degli altri ospiti presenti alla festa erano stati oscurati – si inseriva, infatti,

nell'ambito di un dibattito sui criteri in base ai quali vengono corrisposti contributi e altre utilità pubbliche a privati e aveva lo scopo di documentare l'esistenza di frequentazioni, anche di natura non professionale, tra l'esponente politico ritratto e i segnalanti (l'uno, presidente della Associazione italiana per lo sviluppo e la promozione del digitale terrestre, l'altra, amministratrice di un consorzio assegnatario di un'autorizzazione pubblica per l'utilizzo del digitale terrestre) (nota 28 marzo 2013).

Il Garante ha invece ritenuto travalicati i limiti della libertà di espressione in relazione alla diffusione in rete del contenuto di *e-mail* private, presumibilmente copiate da *hacker*, di alcuni parlamentari. L'Autorità ha rilevato come tale condotta potesse determinare una violazione della libertà e segretezza della corrispondenza (art. 15 Cost.) e delle specifiche garanzie poste a tutela delle comunicazioni e della corrispondenza dei membri del Parlamento (art. 68 Cost.) nonché la configurabilità del reato di cui all'art. 616 c.p. È stata altresì evidenziata una lesione del diritto alla riservatezza e alla protezione dei dati personali non solo dei parlamentari intestatari degli indirizzi di posta elettronica, ma di tutti coloro che sono entrati in contatto con essi attraverso la posta elettronica nonché dei terzi citati all'interno delle comunicazioni.

Il Garante, avendo individuato nella fattispecie un trattamento illecito ritenuto essere avvenuto *ab origine* in violazione di legge (art. 11, comma 1, lett. *a*) e *b*), del Codice) ed avendo rilevato che tale illiceità estendeva i suoi effetti anche ai successivi trattamenti (art. 11, comma 2, del Codice), ha vietato ogni ulteriore utilizzo delle *e-mail* in questione, prescrivendone la cancellazione (provv. 6 maggio 2013, n. 229, doc. web n. 2411368).

9.4. *L'uso di immagini in ambito giornalistico*

Su richiesta dell'Ufficio, talune testate *online* hanno rimosso i video con i quali, in un caso, si documentava la tragica morte di due operai impegnati nella manutenzione di una chiusa e, nell'altro si ritraeva il corpo senza vita di un uomo suicida (di cui erano state rese note generalità e informazioni relative allo stato di salute). In entrambi i casi l'Ufficio ha motivato la richiesta ritenendo non giustificata la diffusione delle immagini sul piano dell'essenzialità dell'informazione a fronte della legittima aspettativa di riserbo e di rispetto del dolore da parte dei familiari delle persone decedute (note 11 e 31 ottobre 2013).

Tutela dei dati idonei a rivelare lo stato di salute

L'Ufficio ha altresì ritenuto fondata la segnalazione di una donna (affetta da una grave patologia) in relazione ad un articolo che, nel documentare la decisione del giudice che aveva riconosciuto sussistente nel caso che riguardava la stessa un episodio di malasanità, aveva diffuso un insieme di dati (professione dell'interessata e la circostanza che fosse affetta da un'evidente menomazione fisica, professione del marito e composizione del nucleo familiare) i quali, nel loro complesso, consentivano di risalire all'identità della segnalante. L'Autorità ha precisato che, anche se l'identificabilità era avvenuta entro una cerchia ristretta di persone, queste ultime erano state comunque messe in condizione di conoscere informazioni sul suo stato di salute (che la segnalante aveva interesse a non rivelare). Nell'occasione è stato ribadito che il limite dell'"essenzialità dell'informazione" va interpretato con particolare rigore quando la notizia di cronaca investe fatti che incidono sulla salute di una persona "identificata o identificabile", richiamando anche la previsione del codice di deontologia secondo cui "il giornalista, nel far riferimento allo stato di salute di una determinata persona, identificata o identificabile, ne rispetta la dignità, il diritto alla riservatezza e al decoro personale, specie nei casi di malattie gravi o terminali, e si astiene dal pubblicare dati analitici di interesse strettamente clinico" (art. 10, comma 1) (nota 1° agosto 2013).

Analogamente è stata ritenuta fondata la doglianza di una donna che aveva lamentato una violazione della sua riservatezza da parte di un giornale locale che, nel riferire del decesso del fratello a causa di una grave malattia, aveva altresì rivelato (senza che ciò fosse pertinente) analoga seria patologia di cui la stessa era affetta (nota 12 marzo 2013).

9.5. *Gli archivi storici e le informazioni* online

Anche nel 2013 sono pervenute segnalazioni e ricorsi concernenti la reperibilità, a distanza di anni, tramite gli archivi storici *online* dei giornali, di dati personali a suo tempo pubblicati. Il Garante ha ribadito che la diffusione sul sito internet di un quotidiano *online* di un articolo contenente informazioni su fatti (anche molto delicati e risalenti) costituisce parte integrante dell'archivio storico della testata e non integra, in linea di principio, un illecito trattamento di dati personali. Tuttavia, tenuto conto del funzionamento della rete – che consente la diffusione di un gran numero di dati personali relativi a vicende anche remote – e in considerazione del tempo trascorso, ha ritenuto che una perenne associazione all'interessato della vicenda resa pubblica possa determinare un sacrificio sproporzionato dei suoi diritti. È stato quindi prescritto che la pagina web contenente i dati personali del ricorrente (anzitutto il suo nominativo) venisse deindicizzata, sottratta cioè alla diretta individuazione da parte dei comuni motori di ricerca, pur restando inalterata all'interno dell'archivio e consultabile telematicamente accedendo all'indirizzo web dell'editore (provv. 18 dicembre 2013, n. 594, doc. web n. 2957346) (cfr. par. 16.4).

In relazione ad un articolo contenente i dati identificativi dell'interessata (rimasta invalida a seguito di un intervento chirurgico) unitamente alla descrizione dettagliata delle relative patologie invalidanti, non rilevanti ai fini del diritto di cronaca, il Garante ha prescritto (con conseguente adempimento da parte dell'editore) la rimozione dell'articolo dagli archivi *online* (provv. 12 dicembre 2013, n. 578, doc. web n. 296950).

In altra fattispecie, vari siti internet e *blog*, dopo aver diffuso articoli relativi ad un collaboratore di giustizia, associando la nuova identità dallo stesso assunta quale effetto dell'adesione al programma di protezione a quella originaria, hanno provveduto ad eliminare tale associazione a seguito dell'intervento dell'Ufficio (nota 20 settembre 2013).

Si segnala, infine, il provvedimento adottato dal Garante il 21 novembre 2013, n. 516 (doc. web n. 2914227) ad esito di un ricorso, avente ad oggetto la richiesta di deindicizzazione dai motori di ricerca del testo di un'interrogazione parlamentare contenente dati giudiziari riferiti al ricorrente (molto risalenti nel tempo e superati da successivi sviluppi processuali) (cfr. par. 16.4).

9.6. *La persistente rintracciabilità sui motori di ricerca*

Ulteriori interventi dell'Autorità si sono resi necessari per assicurare il rispetto dei provvedimenti con cui era stato imposto il divieto di indicizzazione delle notizie contenute negli archivi *online*.

È stato più volte segnalato all'Autorità che, nonostante l'adozione di tutte le misure tecniche previste, alcuni contenuti, apparentemente non più indicizzabili, risultavano visualizzabili nell'indice di *Google search*. Nel novembre del 2013 l'Ufficio ha quindi chiesto, mediante contatti informali, chiarimenti a Google per meglio comprendere e individuare gli strumenti necessari per assicurare la definitiva deindicizzazione dei contenuti rinvenibili tramite il suo motore di ricerca e mira a definire tale aspetto nell'anno in corso, in modo tale da rendere possibilmente più chiara la *policy privacy* della società americana sul punto.

10 Il trattamento di dati personali attraverso internet e nel settore delle comunicazioni elettroniche

10.1. *L'utilizzo dei* cookie*: la consultazione pubblica e il tavolo di lavoro*

Nella Relazione 2012 sono state descritte le modifiche apportate alla disciplina relativa all'uso dei cd. *cookie* (i piccoli *file* di testo che i siti visitati dall'utente inviano al suo *browser* per essere poi ritrasmessi ai medesimi siti alla successiva visita del medesimo utente) e degli altri strumenti analoghi (*web beacon/web bug, clear* GIF, *etc.*) ad opera del d.lgs. 28 maggio 2012, n. 69, che ha novellato l'art. 122 del Codice in attuazione della direttiva 2009/136/CE.

Conclusasi la consultazione pubblica avviata dal Garante (con provv. 22 novembre 2012, n. 359, doc. web n. 2139697) al fine di individuare le modalità semplificate per l'informativa da rendere *online* sull'utilizzo dei *cookie* ai sensi dell'art. 13, comma 3, del Codice, l'analisi dei contributi pervenuti ha evidenziato non solo l'importanza dei menzionati dispositivi per la realizzazione della pubblicità *online* (tramite la profilazione degli utenti), ma anche per il funzionamento dei servizi offerti sulla rete. L'analisi delle problematiche emerse dalla consultazione ha indotto l'Autorità – in ragione della delicatezza della questione e dell'impatto della relativa disciplina sulla rete internet – ad avviare un tavolo di lavoro in materia (riunitosi per la prima volta il 18 settembre 2013) al quale sono stati invitati i partecipanti alla consultazione pubblica nonché esponenti del mondo accademico e della ricerca.

Gli ulteriori elementi acquisiti (anche all'esito di un incontro tenutosi presso l'Autorità nel febbraio 2014) sono attualmente al vaglio dell'Ufficio al fine di individuare le soluzioni giuridiche e tecniche idonee a garantire l'attuazione della normativa in materia.

10.2. *La conservazione dei dati di traffico* (data retention)

Nel 2013 si sono conclusi i procedimenti avviati a seguito del ciclo ispettivo effettuato dal Nucleo speciale *privacy* della Guardia di finanza in materia di conservazione di dati di traffico telefonico e telematico (di cui si è dato conto nella Relazione 2012, p. 259), volti alla verifica del rispetto delle prescrizioni impartite con il provvedimento generale del 17 gennaio 2008 (doc. web n. 1482111) integrato con successivo provvedimento generale del 24 luglio 2008 (doc. web n. 1538237), resosi necessario a seguito del recepimento della direttiva 2006/24/CE sulla conservazione dei dati di traffico mediante il d.lgs. 30 maggio 2008, n. 109 (che ha modificato, tra l'altro, l'art. 132 del Codice).

Rilevata, in sede di accertamento ispettivo, la mancata attuazione di alcune delle prescrizioni contenute nel menzionato provvedimento del luglio 2008, in considerazione delle criticità emerse le società hanno modificato le proprie procedure al fine di assicurare il rispetto della normativa in materia; in qualche caso, a seguito dell'adozione da parte del Collegio di provvedimenti prescrittivi, si sono adeguate nei termini previsti. In particolare, nei confronti di quattro società sono stati adottati provvedimenti prescrittivi per violazioni che hanno riguardato i tempi di conservazione

dei dati di traffico telefonico, superiori a quelli consentiti dalla legge – ed in relazione ai quali, a tacere di altri profili, si è incentrata la declaratoria di invalidità della Corte di giustizia dell'8 aprile 2014 (*Digital Rights Ireland* e *Seitlinger and Others*, Cause riunite C-293/12, C-594/12) – la mancata adozione di specifici sistemi di autenticazione informatica fondati su tecniche di *strong authentication*, di cui una necessariamente basata sull'elaborazione di caratteristiche biometriche dell'incaricato nonché la mancata adozione di alcune ulteriori misure di sicurezza. Tra queste, in particolare, la cifratura dei dati conservati, l'adozione di sistemi informatici disgiunti fisicamente per la conservazione dei dati per esclusive finalità di accertamento e repressione dei reati rispetto a quelli conservati per altre finalità, l'adozione di specifiche procedure in grado di garantire la separazione rigida delle funzioni tecniche di assegnazione di credenziali di autenticazione e di individuazione dei profili di autorizzazione rispetto a quelle di gestione tecnica dei sistemi e della basi di dati (provv.ti 14 febbraio 2013, n. 64, doc. web n. 2313961; 21 febbraio 2013, n. 74, doc. web n. 2338534; 18 luglio 2013, n. 360, doc. web n. 2605222; 3 ottobre 2013, n. 429, doc. web n. 2740948).

In una delle fattispecie esaminate l'istruttoria è stata estesa dall'Ufficio con l'adozione di un ulteriore provvedimento prescrittivo relativo a violazioni della disciplina in materia di protezione dei dati personali concernenti il rilascio di un'informativa inidonea e le non corrette modalità di acquisizione del consenso (specifico e differenziato) da parte degli interessati (provv. 3 ottobre 2013, n. 430, doc. web n. 2745497).

All'attività ispettiva e ai conseguenti provvedimenti prescrittivi adottati dal Collegio ha fatto seguito l'avvio di numerosi procedimenti sanzionatori (cfr. par. 18.5).

10.3. *Le chiamate indesiderate effettuate per finalità promozionali* (*cd.* telemarketing *selvaggio*)

Alla modifica normativa che ha istituito il Registro pubblico delle opposizioni (d.P.R. n. 178/2010) ha corrisposto un incremento delle segnalazioni concernenti la ricezione di chiamate indesiderate sia nei confronti di utenze iscritte regolarmente al Registro (circa 2.300 segnalazioni), sia verso utenze a carattere riservato, in quanto non presenti negli elenchi, ivi comprese le utenze mobili.

Effettuate complesse attività istruttorie, anzitutto per determinare gli effettivi autori delle telefonate (essendo spesso oscurato il numero chiamante: *calling line identification*), si è potuto constatare che molti operatori economici si sono avvalsi, oltre che del proprio personale, anche di terzi i quali, a cascata, hanno ulteriormente demandato l'attività di contatto ad altri soggetti, talora stabiliti all'estero. Nell'insieme, l'esito dei suddetti accertamenti sul solo fenomeno delle chiamate indesiderate ha comportato in meno di tre anni (2011-2013) la contestazione di rilevanti sanzioni amministrative (cfr. par. 18.5).

Il fenomeno del *telemarketing*, con specifico riguardo alle sole segnalazioni relative al detto Registro (escludendo quindi, quelle relative a numerazioni non in elenco), ha fatto registrare una crescita esponenziale delle segnalazioni (circa 2.300 solo nell'anno 2013), larga parte delle quali è riferibile a più chiamate promozionali ascrivibili a prodotti e servizi commercializzati dalla medesima impresa. Al fine di offrire un'ampia tutela agli interessati e contrastare efficacemente il fenomeno (oggetto di ricorrente segnalazione), l'Autorità ha spesso avviato singole istruttorie preliminari (anche in mancanza dell'indicazione da parte del segnalante del numero chiamante).

10.4. *Le nuove regole per il contrasto alle cd. telefonate mute effettuate da* call center *con finalità di* marketing

Si è ampiamente riferito nella Relazione 2011 (p. 104 e ss.) delle telefonate cd. mute, ovvero effettuate mediante un sistema automatizzato per la generazione delle chiamate dirette agli abbonati telefonici che consente di mantenere in uno stato di attesa le chiamate che hanno già ricevuto risposta, suscettibili, quindi, di ingenerare allarme, ansia, sospetto e disturbo nei destinatari, fino al momento in cui un operatore di *call center* si rende disponibile.

In proposito merita segnalare che un primo provvedimento adottato dal Garante (provv. 6 dicembre 2011, n. 474, doc. web n. 1857326), oggetto di impugnazione, è stato integralmente confermato dal Tribunale di Roma (con sentenza n° 18977 depositata il 26 settembre 2013). In particolare, il giudice ha accolto la tesi del Garante stabilendo che "l'utilizzo dei dati personali per effettuare una chiamata muta in luogo che una proposta commerciale costituisce un trattamento di dati contrario al fondamentale canone della correttezza indicato dall'articolo 11 del Codice, atteso che tutto il sistema di selezione e formulazione delle chiamate [...] mira ad ottimizzare il successo delle chiamate passare agli operatori facendo ricadere il rischio e il disagio della chiamata muta sui destinatari".

Il fenomeno in esame ha peraltro fatto registrare un significativo incremento, specie negli ultimi mesi (alla fine del 2013, risultano pervenute circa 400 segnalazioni, alcune peraltro singolarmente riferibili a più episodi, anche ascrivibili a soggetti diversi), nonché la tendenza ad allarmanti picchi di chiamate mute effettuate da specifiche numerazioni in periodi di tempo determinati. Dalle verifiche e dagli approfondimenti conoscitivi effettuati, anche di carattere ispettivo, è emerso che in tutti i casi oggetto di segnalazione si trattava di telefonate effettuate da *call center* per finalità commerciali mediante l'impiego, ormai diffusissimo, di sistemi automatizzati di instradamento della chiamata agli operatori. Nella maggior parte dei casi le liste dei destinatari delle chiamate commerciali vengono "caricate" sulla piattaforma informatica utilizzata dai *call center* la quale, mediante l'impiego di un *software*, compone i numeri e smista le telefonate ai diversi operatori.

Con decisione n. 482 del 30 ottobre 2013 (doc. web n. 2740497) l'Autorità ha posto in consultazione pubblica per 60 giorni (dandone avviso sulla G.U. del 22 novembre 2013, n. 274) uno schema di provvedimento generale che individua una serie di misure per rendere il trattamento conforme alle disposizioni del Codice. In tale prospettiva, in particolare: 1) i *call center* dovranno censire correttamente e secondo criteri uniformi le chiamate mute effettuate agli interessati, la cui attesa non potrà prolungarsi oltre i 3 secondi, intervallo temporale oltre il quale la chiamata dovrà essere "abbattuta" dal sistema; 2) il numero di chiamate mute considerate entro la soglia di tollerabilità fisiologica non potrà essere superiore al 3% di tutte le chiamate andate a buon fine; tale percentuale dovrà essere misurata ad intervalli decadali e comunque nell'ambito di ogni singola campagna di *telemarketing*; 3) alla risposta dell'utente non potrà mai far riscontro il silenzio, che dovrà invece essere sostituito da un rumore sintetico ambientale (cd. *comfort noise*) con rumori di sottofondo, squilli di telefono, brusio, *etc.*, per dare la sensazione che la chiamata non provenga da molestatori; 4) a seguito di una chiamata muta, l'utente non potrà essere ricontattato prima di una settimana e comunque al contatto successivo dovrà essere prevista una modalità di instradamento automatico della chiamata stessa in modo da assicurare la presenza di un operatore; 5) i *call center* dovranno conservare per almeno due anni i *report* statistici della chiamate mute effettuate, in modo da consentire gli opportuni controlli.

10.5. *Il trattamento di dati personali effettuato mediante* call center *ubicati al di fuori dell'Unione europea*

Il trasferimento di molte attività verso *call center* insediati in Paesi non appartenenti all'Unione europea, nei quali potrebbero non essere assicurate le adeguate garanzie per i diritti degli interessati previste dalla normativa comunitaria, ha messo in luce possibili criticità sulle modalità di trattamento dei dati. Già a partire dal 2010, la questione della delocalizzazione all'estero delle attività di *call center* è stata riportata da diverse fonti di stampa e segnalata al Garante da strutture sindacali e associazioni di consumatori.

Successivamente, come noto, l'art. 24-*bis*, d.l. 22 giugno 2012, n. 83 convertito con modificazioni, dalla l. 7 agosto 2012, n. 134 (in G.U. 11 agosto 2012, n. 187), ha prescritto alle imprese che intendano spostare la propria attività al di fuori del territorio nazionale di darne previa comunicazione al Ministero del lavoro e delle politiche sociali e al Garante, stabilendo altresì che gli interessati, nel rivolgersi a (o se contattati da) un *call center*, siano sempre informati del fatto che l'operatore possa essere collocato in un Paese estero. Sono al riguardo pervenute, da parte delle imprese e delle associazioni di categoria, richieste di chiarimenti nonché di intervento del Garante per verificare le modalità di trattamento.

Nel contempo la Commissione europea è intervenuta nei confronti dell'Italia con una richiesta di informazioni, trasmessa al Garante dalla Presidenza del Consiglio dei Ministri, volta a verificare la sussistenza di eventuali presupposti per un'infrazione comunitaria in conseguenza delle possibili antinomie rilevate nel citato art. 24-*bis*, con particolare riguardo alla restrizione della libertà di srabilimento che l'applicazione della norma comporterebbe. Al riguardo sarebbe auspicabile un tempestivo intervento del legislatore tale da assicurare, in ragione di rilievi sollevati una formulazione della norma coerente con il diritto comunitario.

Con il provvedimento del 10 ottobre 2013, n. 444 (doc. web n. 2724806) il Garante ha comunque fornito indicazioni e chiarimenti, per i profili di propria competenza, anche in relazione agli strumenti da adottare per trasferire lecitamente dati personali verso Paesi terzi nonché sugli adempimenti espressamente previsti dall'art. 24-*bis*, prescrivendo ai titolari del trattamento di comunicare all'Autorità ogni trasferimento o affidamenro di dati personali a *call center* siti al di fuori dell'Unione europea; ciò anche al fine di consentire all'Autorità di effettuare una ricognizione del fenomeno disponendo di dati completi che riguardino tutti i settori pubblici e privati coinvolti, nonché per arginare efficacemente il fenomeno delle chiamate indesiderate.

Rispetto alle poco meno di 40 notificazioni ad oggi pervenute l'Autorità, pur non avendo ricevuto segnalazioni, ha tuttavia programmato un'attività ispettiva *ad hoc* per il 2014 al fine di verificare in concreto il rispetto delle vigenti disposizioni.

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

Con riguardo ai trattamenti effettuati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico per finalità di profilazione della propria clientela attraverso l'uso di dati personali aggregati e senza l'acquisizione dello specifico consenso, il Garante ha analizzato una nuova istanza di verifica preliminare pervenuta da parte di un operatore telefonico sulla base del provvedimento generale del 25 giugno 2009 (doc. web n. 1629107). All'esito della stessa, l'Autorità ha emanato un provvedimento con il quale, nel prescrivere misure e accorgimenti (sia giuridici,

sia tecnici) volti a garantire, nell'ambito dell'attività di profilazione, il corretto utilizzo dei dati personali degli utenti ed a rafforzarne la tutela (provv. 24 ottobre 2013, n. 468, doc. web n. 2797824), si è consentito all'operatore telefonico in questione, previa adozione di rigorose misure di sicurezza, di ampliare i parametri utilizzati per la definizione della propria clientela e conseguentemente per la definizione di più idonei *cluster* (gruppi omogenei) di utenza sui quali articolare l'attività di profilazione. Inoltre, a fronte delle difficoltà rappresentate dall'operatore con riguardo ad una corretta ed adeguata gestione dei cicli di fatturazione, e soprattutto al fine di tutelare gli utenti a cui potevano essere imputati comportamenti di consumo non veritieri, l'Autorità ha anche autorizzato un'estensione del periodo di riferimento utilizzato per l'elaborazione del criterio di ripartizione della clientela nei suddetti *cluster*. Al fine di garantire gli utenti, l'Autorità non ha ritenuto invece lecita una nuova modalità di profilazione ipotizzata, nell'ambito di un'istanza di verifica preliminare, da una società di telecomunicazioni sulla base del monitoraggio dei dati di navigazione degli stessi (provv. 13 giugno 2013, n. 300). L'attività sottoposta al vaglio del Garante riguardava la cosiddetta pubblicità comportamentale (*targeted advertising*) e i servizi personalizzati su internet. La società fornitrice del servizio di connessione chiedeva infatti di poter analizzare il comportamento *online* degli utenti, senza averne acquisito il consenso, al fine di proporre pubblicità mirate (*targeted advertising*). Diversamente da quanto prospettato, è tuttavia emerso che il processo che avrebbe dovuto rendere anonimi i dati dei singoli utenti era, per sua natura, reversibile e consentiva di proporre all'utente offerte calibrate sulla sua condotta *online*.

Alla medesima società l'Autorità ha consentito, invece, nell'ambito di un'ulteriore istanza di verifica preliminare relativa alla fornitura di servizi di tv interattiva, di analizzare, previa acquisizione del consenso, il comportamento degli utenti e, in particolare, preferenze, gusti e scelte di consumo sui servizi e prodotti fruibili attraverso le piattaforme televisive digitali ed internet (provv. 11 aprile 2013, n. 177). A tal fine, sono state prescritte misure a tutela della riservatezza degli interessati, quali l'esclusione, per finalità di profilazione e *marketing*, dell'analisi di dati sensibili, a meno che il trattamento di tali dati non risultasse indispensabile in rapporto ad uno specifico bene o prodotto richiesto o, ancora, l'adozione, nella fase di classificazione dei prodotti televisivi fruibili in modalità interattiva, di una più ampia categorizzazione dei contenuti per genere (e che comunque non si riferisse a singole tipologie di contenuti digitali) nonché la previsione di un periodo di osservazione di gusti e preferenze di consumo non inferiore alla settimana.

Nel corso dell'istruttoria è emerso, inoltre, che la società avrebbe utilizzato, per l'analisi delle abitudini di consumo dei clienti della tv interattiva, la medesima piattaforma *software* usata per i servizi di telefonia e di profilazione telefonica. Pertanto, al fine di scongiurare i rischi di una "profilazione incrociata", il Garante ha prescritto il mascheramento dei dati personali all'interno dei diversi sistemi (provv. 11 aprile 2013, cit.).

10.7. *Il trattamento dei dati personali per finalità di* marketing *diretto: la manifestazione del consenso*

Dopo una articolata attività istruttoria volta a verificare la liceità e la correttezza dei trattamenti effettuati dai maggiori operatori nazionali di telefonia con riguardo ai dati personali dei clienti acquisiti sulla base del consenso (manifestato all'atto della sottoscrizione di un contratto di abbonamento o dell'attivazione di una linea prepa-

gata), il Garante è intervenuto con un provvedimento generale (15 maggio 2013, n. 242, doc. web n. 2543820) in tema di manifestazione del consenso nell'ambito del cd. *marketing* diretto; con esso sono state dettate alcune prescrizioni, successivamente ribadite con le linee guida in materia di attività promozionale e contrasto allo *spam* del 4 luglio 2013 (di cui, più nel dettaglio, v. *infra* par. 10.10). In particolare, con il menzionato provvedimento del 15 maggio 2013 – che (pur originato nel contesto degli operatori telefonici) si rivolge a tutti i titolari che effettuano trattamenti di dati personali in ambito privato – l'Autorità ha delineato, nel rispetto dei principi di semplificazione, armonizzazione ed efficacia di cui all'art. 2, comma 2, del Codice, una linea interpretativa dell'art. 130, commi 1 e 2, del Codice in relazione al disposto dell'art. 23, tesa a semplificare l'acquisizione del consenso dell'interessato per l'attività di *marketing* diretto attraverso strumenti tradizionali e automatizzati di contatto (posta elettronica, telefax, messaggi del tipo mms o sms o di altro tipo). In particolare, il Garante ha chiarito che l'acquisizione del consenso degli interessati per il trattamento dei dati personali per finalità di *marketing* diretto (ossia per l'invio di materiale pubblicitario, di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale), tramite modalità automatizzate ai sensi dell'art. 130, commi 1 e 2, del Codice, implica altresì il consenso alla ricezione di comunicazioni promozionali attraverso modalità tradizionali, come la posta cartacea o le chiamate telefoniche tramite operatore, salvo l'esercizio da parte dell'interessato del diritto di opposizione al trattamento (anche in forma parziale, limitatamente a talune modalità dell'attività di *marketing*).

Il Garante ha inoltre chiarito che dall'informativa deve emergere che il diritto di opposizione dell'interessato al trattamento per finalità di *marketing* diretto attraverso modalità automatizzate si estende a quelle tradizionali, anche se deve comunque restare salva la possibilità di esercitare tale diritto in parte, così come previsto dal citato art. 7, comma 4, del Codice. La stessa informativa deve infatti evidenziare la possibilità per l'interessato di manifestare comunque in maniera agevole e gratuita l'eventuale volontà di ricevere comunicazioni promozionali esclusivamente attraverso modalità tradizionali, ove previste. L'Autorità ha infine prescritto ai titolari del trattamento che per le menzionate finalità abbiano già raccolto un unico consenso con riguardo a comunicazioni sia automatizzate sia tradizionali, di inserire un analogo richiamo alla suddetta possibilità in un'informativa da rendere alla prima occasione utile, eventualmente anche mediante le ordinarie modalità di contatto per scopi endocontrattuali.

Con lo scopo di chiarire l'ambito di un corretto trattamento dei dati personali anche rispetto alla formulazione di una modulistica relativa sia all'informativa (*ex* art. 13 del Codice), sia al consenso (*ex* art. 23 del Codice) in termini selettivi, ovvero che consenta di prestare un consenso specifico per ogni finalità perseguita dal titolare, l'Autorità è intervenuta anche con riguardo ai trattamenti di dati personali svolti per finalità di *marketing* diretto da società che operano nel settore dei finanziamenti privati. In tale ambito, con riguardo alla comunicazione dei dati a soggetti terzi sempre per finalità di *marketing*, l'Ufficio, per garantire agli interessati confini più chiari dell'ambito in cui i loro dati vengono trattati, ha rilevato che il titolare, nel rendere un'idonea informativa, circa gli elementi di cui al citato art. 13, deve indicare, ove opportuno, tra i soggetti terzi destinatari della comunicazione anche le società controllate, controllanti o comunque a vario titolo collegate con il soggetto che ha raccolto i dati, ovvero, in alternativa le categorie merceologiche di appartenenza dei suddetti terzi (note 3 e 12 dicembre 2013).

10.8. *Il* mobile payment

Come riferito nella Relazione 2012, il Garante ha avviato un'attività conoscitiva in merito ai nuovi servizi di pagamento attraverso il telefono cellulare, noti come *mobile remote payment*, che vedono coinvolti, in particolare, operatori di telecomunicazioni, *hub* tecnologici e fornitori di beni e servizi digitali, che, tramite applicazioni che consentono l'accesso a un mercato virtuale, offrono agli utenti la possibilità di acquistare servizi e prodotti digitali fruibili tramite *smartphone*, PC e *tablet*, con addebito del relativo costo sul conto telefonico ovvero con decurtazione dell'importo dal credito telefonico (nel caso di *sim* ricaricabili).

All'esito di tale attività, con provvedimento del 12 dicembre 2013, n. 561, è stata avviata una pubblica consultazione su uno schema di provvedimento generale in materia (doc. web n. 2830145) volto a garantire, in un mercato sempre più dinamico, un uso sicuro e corretto delle informazioni che riguardano gli utenti alla luce dell'attuale assetto normativo del settore (cfr. in particolare la direttiva sui servizi di pagamento 2007/64/CE, cd. *Payment Service Directive*, il relativo decreto di recepimento, d.lgs. 27 gennaio 2010, n. 11, e il provvedimento della Banca d'Italia del 5 luglio 2011 "Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 relativo ai servizi di pagamento").

L'attività conoscitiva si è estesa anche ai *server* di *mobile proximity payment* che riguardano le operazioni di pagamento di beni (digitali e non) eseguite dal cliente avvicinando il dispositivo mobile, dotato di tecnologia NFC (*Near Field Communication*) che fornisce connettività *wireless* (RF) bidirezionale a corto raggio, ad un apposito lettore pos (*point of sale*) posto presso il punto vendita dell'esercente da cui si acquista il bene. Tali servizi sono offerti da soggetti che operano in ambito bancario e nel circuito delle carte di credito.

In tale ambito, il Garante si è quindi riservato, all'esito di tale attività, di intervenire, nei limiti delle proprie competenze, con ulteriori provvedimenti che potranno investire anche il settore dell'offerta e dei pagamenti di titoli digitalizzati per l'accesso a servizi di utilità sociale o a servizi in mobilità (con riguardo, in particolare, alle operazioni di *mobile ticketing* e *mobile parking*).

10.9. *La disciplina dei* data breach

Gli obblighi per i fornitori di servizi di comunicazione elettronica accessibili al pubblico (quali telefonia, accesso a internet, *account* di posta elettronica, *etc.*) di comunicare le violazioni di dati personali ai sensi del nuovo testo degli artt. 32 e 32-*bis*, del Codice sono già stati ampiamente descritti nella Relazione 2012 (v. p. 171 e ss.) unitamente alle "Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali" (provv. 26 luglio 2012, n. 183, doc. web n. 1915485), contenenti prescrizioni nei confronti dei fornitori; l'Autorità ha altresì predisposto un modello per la comunicazione dei *data breach* (reso disponibile *online* sul sito dell'Autorità: cfr. doc. web n. 1915835).

All'esito della consultazione pubblica avviata nel 2012, in merito ad alcune specifiche modalità applicative della nuova disciplina contenuta nell'art. 32-*bis* del Codice (e in considerazione dei primi casi di violazione di dati personali comunicati dai fornitori), il Garante ha adottato, ai sensi dell'art. 32-*bis*, comma 6, del Codice, un provvedimento generale – che ha sostituito le ricordate linee guida – per fornire indicazioni in relazione alle circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione e alle relative modalità di effettuazione (provv. 4 aprile 2013, n. 161, doc. web n. 2388260).

Nel redigere tale provvedimento, l'Autorità ha tenuto conto delle indicazioni della Commissione europea, formalizzate poi nel regolamento Ue n. 611/2013 del 24 giugno 2013, sulle misure applicabili alle comunicazioni dei *data breach* (in G.U.E.E. n. L 173 del 26 giugno 2013 ed entrato in vigore il 25 agosto 2013), sì da rendere sostanzialmente omogenei i due atti (che presentano lievi differenze, attinenti più a profili procedurali che di merito).

Nel 2013 sono pervenute all'Autorità circa venti comunicazioni di *data breach*, da parte dei più importanti fornitori di servizi di comunicazione elettronica operanti in Italia.

In alcuni casi, la violazione ha riguardato i servizi offerti *online* dai fornitori sui propri siti web, quali, ad esempio, quelli che consentono alla clientela di effettuare ricariche telefoniche o visualizzare il traffico telefonico effettuato a fini di controllo dell'esattezza degli addebiti; in tale ambito, gli incidenti verificatisi hanno determinato la visualizzazione, da parte di alcuni clienti, di dati relativi ad altri interessati (quali, ad es., i numeri dei clienti che hanno effettuato la ricarica, l'ammontare della stessa nonché i numeri in uscita dall'utenza coinvolta).

In un caso, che ha riguardato uno dei principali ISP italiani, un utente, accedendo alla propria *webmail*, ha visualizzato la *mailbox* di un altro utente (che a sua volta aveva perso alcuni messaggi di posta elettronica). Entrambi si erano prontamente rivolti al gestore che, oltre a recuperare quasi tutti i messaggi perduti, ha chiarito la natura dell'anomalia verificatasi.

In un altro caso, l'Autorità si è attivata sulla base delle notizie, apparse su diversi mezzi di informazione, relative ad un attacco informatico che aveva minato la sicurezza degli indirizzi *e-mail* e delle *password* di circa 250.000 utenti di un noto *social network*. È stata così inviata una dettagliata richiesta di informazioni alla società statunitense che lo gestisce, che ha fornito gli elementi richiesti assicurando, peraltro, di aver notificato l'accaduto alle competenti autorità federali e di avere in corso ulteriori accertamenti, con la collaborazione delle stesse, nonché di aver subito modificato le *password* degli utenti coinvolti mettendoli al corrente dell'accaduto tramite messaggi di posta elettronica.

Il pregiudizio per i dati personali degli utenti è derivato, in alcuni casi, dalle incaute operazioni svolte dagli stessi e non dalla negligenza dei fornitori. Il Garante, ad esempio, ha verificato, mediante accertamento ispettivo, il furto delle credenziali di autenticazione di clienti di una società di telecomunicazioni, effettuato attraverso l'installazione operata dagli stessi clienti sui propri terminali mobili, di un'*app* fraudolenta tramite la quale ignoti carpivano le suddette credenziali e le utilizzavano per attività di *spam*.

Nei casi sinora esaminati, l'Autorità, all'esito delle istruttorie svolte nei confronti dei fornitori, ha verificato che fossero state adottate misure idonee a porre rimedio alle violazioni subite e a prevenirne di analoghe. In nessuno dei casi trattati si è ritenuto necessario adottare uno specifico provvedimento. Tuttavia, nell'ambito dell'istruttoria relativa ad una specifica violazione comunicata all'Autorità, è stata rilevata l'inosservanza, da parte del fornitore, dei ristretti termini per la comunicazione al Garante (24 ore dall'avvenuta conoscenza della violazione per la prima sommaria comunicazione e 3 giorni da questa per la comunicazione dettagliata) ed è stato pertanto avviato un separato procedimento sanzionatorio.

Oltre alla gestione ordinaria delle comunicazioni di *data breach*, l'Autorità ha partecipato agli approfondimenti svolti sulla materia a livello europeo, anche al fine di assicurare l'uniformità delle misure in vigore nei diversi Paesi. I temi di maggiore rilievo affrontati in quest'ambito sono stati: il canale predisposto presso le diverse autorità competenti per le comunicazioni di *data breach*; la collaborazione tra le diverse

autorità nazionali competenti nei casi di violazioni che riguardino interessati situati in diversi Stati membri nonché la valutazione da parte delle autorità competenti delle misure tecnologiche adottate dai fornitori per far fronte alle singole violazioni, con particolare riferimento all'ininrelligibilità dei dati.

10.10. *Il contrasto allo* spam

L'Autorità ha proseguito l'arrività di contrasto al fenomeno dello *spam* (v. *infra* più nel derraglio, le linee guida del 4 luglio 2013, n. 330, doc. web n. 2542248).

Turtavia, anche nel 2013 numerose sono state le segnalazioni telarive a sms, fax e ancor più *e-mail* indesiderati, per le quali talvolta è risultato difficile individuare i titolari del trarramento, sia per la modalirà con cui si può operare in tete, sia perché talora i siti "mittenti" risultano inrestati a soggetti fantasiosi o comunque privi di recapiti utilmente contattabili (non di rado in Paesi extraeuropei). Quando, invece, l'invio di fax e, ancor più di *e-mail*, promozionali indesiderati è risultato effettuato da società localizzate in Paesi membri dell'Ue (in particolare, Francia, Inghilterra e Germania), il Garante ha richiesto la collaborazione delle competenti Autorità per far cessare gli invii, nei limiti consentiti dalle (diverse) legislazioni esistenti. In proposito, merita segnalare anche che l'Autorirà è designata quale autorità nazionale competente per l'applicazione dell'art. 13 della direttiva 2002/58/CE (relativo alle comunicazioni indesiderate) nell'ambito del Sistema di cooperazione per la tutela dei consumatori (CPCS), creato dal regolamento (CE) n. 2006/2004 al fine di agevolare lo scambio di informazioni e la cooperazione tra le autorità europee competenti in materia di tutela dei consumatori.

Nella maggior parte dei casi, in cui il titolare del trattamento è stato individuato, l'Autorità ha avviato apposite istruttorie preliminari anche in relazione alla singola segnalazione. Talora sono stati ravvisati i presupposti per l'avvio di un autonomo procedimento sanzionatorio nei confronti del medesimo titolare ai fini dell'eventuale applicazione delle sanzioni previste dal Codice, con particolare riferimento alla violazione dell'obbligo dell'informativa ai sensi dell'art. 13 del Codice e dell'obbligo di previa acquisizione del consenso del destinatario delle comunicazioni automatizzate ai sensi degli artt. 23 e 130 del Codice (note 21 maggio e 13 novembre 2013). Più spesso, quando l'invio di comunicazioni promozionali automatizzate è risultato occasionale, oppure frutto di un mero errore, l'Ufficio ha invece inviato ai titolari del trattamento apposite note di richiamo al pieno rispetto della disciplina in materia (note 30 settembre e 28 ottobre 2013).

L'Autorità inoltre è intervenuta per fornire una serie di indicazioni anche agli organismi che si occupano di formazione in materia di mediazione civile e commerciale. In particolare, è stato evidenziato che, in assenza del preventivo consenso dell'interessato, non è possibile inviare comunicazioni tramite modalità automatizzate, neanche nel caso in cui i dati personali siano tratti da registri pubblici, elenchi, siti web, atti o documenti conosciuti o conoscibili da chiunque e i destinatari delle predette comunicazioni siano soggetti che svolgono un'attività economica. Un ulteriore consenso dell'interessato è poi necessario laddove il trattamento implichi la comunicazione di dati a terzi: non è infatti possibile utilizzare sistemi automatizzati di invio di messaggi promozionali, come le *mailing list*, che rendano visibili a tutti i destinatari gli indirizzi di posta elettronica utilizzati, senza rilasciare l'informativa ed acquisire il consenso degli interessati (nota 16 maggio 2013).

Con riferimento alle nuove forme di *spam*, ed in particolare all'attività di *social marketing* (effettuata, nei confronti degli utenti di *Facebook*, *Twitter* e di altri *social network* o mediante servizi di messaggistica e *Voip* sempre più diffusi), è stato ribadito,

da un lato, che l'agevole reperibilità dei dati personali in rete non significa che gli stessi possano essere liberamente usati per inviare comunicazioni promozionali agli interessati; dall'altro, che a questi tipi di trattamento non può essere applicato rigidamente il Codice, soprattutto tenendo conto della peculiare funzione dei *social network*, che comportano la condivisione volontaria e la circolazione di idee e dati personali, nelle forme di conoscenze, foto, contatti, gusti ed *hobby*.

Riguardo a siffatta attività, l'Autorità ha individuato, fra quelle più ricorrenti, due ipotesi. Una prima ipotesi è quella in cui l'utente riceve in bacheca o al proprio indirizzo di posta elettronica (collegato al profilo *social*) un messaggio promozionale (relativo a uno specifico prodotto o servizio) da parte di chi abbia ricavato i menzionati dati di contatto dal profilo del *social network* al quale l'utente è iscritto. Una seconda fattispecie ricorre quando l'utente sia diventato *fan* della pagina di una determinata impresa o società oppure si sia iscritto a un gruppo di *follower* di un determinato marchio, personaggio, prodotto e, in tale veste, riceva quindi messaggi a contenuto promozionale.

Nel primo caso, il trattamento viene considerato illecito, a meno che il mittente non dimostri di aver acquisito dall'interessato un consenso preventivo ai sensi dell'art. 130, commi 1 e 2, del Codice. Nel secondo caso, invece, l'invio di comunicazioni promozionali riguardanti un determinato marchio, prodotto o servizio, effettuato dall'impresa a cui fa riferimento la relativa pagina, può considerarsi lecito se dal contesto o dalle modalità di funzionamento del *social network*, anche sulla base delle informazioni rese, possa desumersi che l'interessato abbia in tal modo voluto fornire il proprio consenso alla ricezione di messaggi promozionali. Venuta meno la qualità di *follower* (o comunque in caso di opposizione al ricevimento di eventuali ulteriori comunicazioni promozionali), il successivo invio di messaggi promozionali sarà illecito, con le relative conseguenze sanzionatorie.

L'Autorità, inoltre, con le linee guida del 4 luglio 2013, ha stabilito che il *marketing* "virale" può rientrare nello *spam* se non rispetta principi e norme, con particolare riferimento agli artt. 3, 11, 13, 23 e 130 del Codice. Non è comunque soggetto al Codice il trattamento dei dati effettuato da chi, ricevendo una proposta promozionale, la inoltri a sua volta a titolo personale, consigliando il prodotto o il servizio ai propri amici, pur utilizzando strumenti automatizzati, come sms o *e-mail* (cd. passaparola); il Codice si applica invece al trattamento effettuato da chi inoltri, o comunque comunichi il messaggio promozionale ricevuto a una molteplicità di destinatari i cui dati personali (numeri di telefono o indirizzi *e-mail*) siano stati reperiti su elenchi pubblici o sul web.

L'Autorità ha infine ricordato che le persone giuridiche (come anche enti e associazioni), sottratte dal campo applicativo del concetto di "interessato", pur non potendo più chiedere l'intervento dell'Autorità nelle forme previste dal Codice (segnalazione, reclamo, ricorso), possono comunque essere indirettamente tutelate dal Garante che, messo a conoscenza, per il tramite di tali soggetti, di possibili violazioni della normativa sulle comunicazioni promozionali automatizzate, può intervenire nell'esercizio dei suoi poteri *ex officio*, inclusi quelli sanzionatori.

10.11. *La profilazione della clientela e i beni di lusso*

Nel 2013 sono stati adottati dal Garante tre provvedimenti prescrittivi, sulla base di altrettante istanze di verifica preliminare presentate all'Autorità da società di alta moda e che offrono beni di lusso finalizzate ad effettuare operazioni di trattamento per profilare la propria clientela ed offrirle servizi personalizzati (cd. *marketing* profilato).

Le richieste sono state presentate dalle società ai sensi dell'art. 17 del Codice, sulla base del provvedimento generale del 24 febbraio 2005 relativo alle carte di fidelizzazione (doc. web n. 1103045), nel quale è previsto che chiunque voglia conservare i dati della propria clientela per finalità di profilazione e *marketing*, per un periodo superiore a dodici mesi, deve presentare al Garante un'istanza di verifica preliminare.

Nelle richieste le società prospettavano un tempo di conservazione pari a dieci anni dei dati personali della clientela, comprensivi del dettaglio degli acquisti effettuati.

Il Garante, ricordando che tali attività necessitano comunque, *in primis*, del consenso (pienamente informato) degli interessati, ha ritenuto congruo un periodo di conservazione pari a sette anni (cfr. provv. 30 maggio 2013, n. 263, doc. web n. 2547834; provv. 7 novembre 2013, n. 500, doc. web n. 2920245) e a dieci anni (in provv. 24 aprile 2013, n. 219, doc. web n. 2499354) – con successiva cancellazione o trasformazione in forma anonima – considerando tra l'altro che i beni acquistati riguardano un genere particolare, di cd. fascia alta, con acquisti effettuati una o due volte l'anno, sicché un periodo inferiore di conservazione avrebbe potuto determinare, nella sostanza, l'impossibilità di profilare la clientela.

Il Garante, in occasione di tali verifiche, ha precisato che ciascun punto vendita deve essere designato come responsabile del trattamento ed ha altresì evidenziato l'esigenza di acquisire apposite procedure di autenticazione ed autorizzazione nonché il tracciamento dei *log* di accesso a ciascun sistema informatico, in modo da realizzare un controllo analitico *ex post* delle attività svolte dai singoli incaricati (provv.ti 24 aprile, 30 maggio e 7 novembre 2013, citati).

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

La materia del trattamento dei dati personali nel settore del lavoro (pubblico e privato) ha registrato, nel periodo considerato, un ulteriore incremento del numero di segnalazioni e reclami pervenuti da parte di singoli o di rappresentanze sindacali per i quali, tenuto conto della necessità dell'accertamento delle circostanze di fatto, non di rado l'Ufficio ha dovuto ricorrere ad attività di natura ispettiva, sovente avvalendosi della Guardia di finanza (cfr. par. 18.2).

Una ricognizione, pur sommaria, delle istanze rivolte all'Autorità – ancorché le annotazioni svolte di seguito si incentrino prevalentemente sui provvedimenti adottati dal Garante – consente di rilevare che, dal punto di vista contenutistico, continuano a pervenire numerose segnalazioni concernenti l'utilizzo dei sistemi più vari che consentono il controllo a distanza dei lavoratori come pure la circolazione dei dati nel contesto lavorativo (tra colleghi come pure verso terzi); un significativo aumento contrassegna le segnalazioni e i quesiti conseguenti alla disciplina di trasparenza in ambito pubblico contenuta nel d.lgs. n. 33/2013, anche in considerazione delle valutazioni critiche espresse dal Garante nel parere rispetto allo schema di decreto trasmesso all'Autorità (provv. 7 febbraio 2013, n. 49: cfr. par. 3.2.2.A), che è altresì tornata a pronunciarsi sull'utilizzo dei dati biometrici al fine di commisurare il tempo di lavoro. Contesto (nuovo rispetto al passato) sul quale l'Autorità è stata chiamata a pronunciarsi (mettendo a parte, per le valutazioni di competenza, il Ministero del lavoro e delle politiche sociali – Direzione generale per le politiche dei servizi per il lavoro della decisione adottata) è quello del trattamento di dati personali di persone che, alla ricerca di un posto di lavoro, ricorrono ai più vari canali di intermediazione e, tra questi, a soggetti che, gestendo siti internet, trattano – specie in considerazione della profonda crisi occupazionale che attraversa il Paese – quantità rilevantissime di dati personali.

Un cenno merita la riproposizione, specie da parte di società multinazionali, della questione inerente le condizioni di liceità del trattamento di dati personali delle persone coinvolte nel funzionamento di procedure di segnalazione interna (cd. *whistleblowing*), tematica che, benché oggetto di segnalazione a Parlamento e Governo da parte dell'Autorità (cfr. provv. 10 dicembre 2009, doc. web n. 1693019), sia in relazione al settore pubblico che a quello privato, ha formato oggetto di intervento regolatorio – con disposizione, contenuta nell'art. 54-*bis*, d.lgs. 30 marzo 2001, n. 165, come novellato dall'art. 1, comma 51, l. 6 novembre 2012, n. 190, che trova espressa applicazione al solo ambito pubblico (lasciando peraltro irrisolti nodi di non poco momento, pur evidenziati nella menzionata segnalazione) –, con conseguente (persistente) incertezza giuridica per gli operatori.

Si segnala inoltre che, a fine 2013, l'autorizzazione generale al trattamento dei dati sensibili nei rapporti di lavoro è stata rinnovata per un altro anno, in termini sostanzialmente analoghi alla precedente (provv. 12 dicembre 2013, n. 564, doc. web n. 2818993).

11.1. *Il trattamento di dati personali e i controlli a distanza*

Videosorveglianza

Una ricognizione più puntuale dei provvedimenti del Garante consente di evidenziare tra le aree di più frequente intervento dell'Autorità – nonostante precedenti ormai copiosi (della giurisprudenza, anzitutto, e quindi del Garante) – quella del trattamento di dati personali mediante strumenti di controllo a distanza, per lo più mediante sistemi di videosorveglianza. In quest'ambito, i provvedimenti che hanno rilevato l'illiceità del trattamento ai sensi dell'art. 11, comma 1, lett. *a*), del Codice, sovente si radicano nell'inosservanza delle garanzie previste dalla disciplina di settore (segnatamente l'art. 4, comma 2, l. 20 maggio 1970, n. 300, richiamato dall'art. 114 del Codice) che, come noto, consistono nel preventivo accordo con le rappresentanze sindacali dei lavoratori rispetto all'installazione delle apparecchiature di controllo o nell'autorizzazione del competente ufficio periferico del Ministero del lavoro (il cui procedimento di rilascio è stato peraltro semplificato con la circolare del 16 aprile 2012, prot. n. 7162 del Ministero del lavoro e delle politiche sociali).

Le fattispecie prese in considerazione hanno riguardato una casistica assai varia, nella quale spiccano (per la gravità delle condotte tenute) alcune vicende nelle quali è stato accertato che la ripresa delle immagini è stata effettuata in modo occulto (violando così anche il principio di correttezza nei trattamenti) e quindi all'insaputa dei lavoratori (cfr. provv. 4 aprile 2013, n. 164, doc. web n. 2439178, nel quale le telecamere sono risultate celate all'interno di rilevatori di fumo e dei segnali luminosi delle uscite di emergenza in una società editoriale) nonché, talvolta, anche della clientela (cfr. provv. 4 aprile 2013, n. 163, doc. web n. 2464167, concernente microcamere occultate nei *privées* di un locale notturno nonché mimetizzate all'interno dei camerini delle dipendenti del locale; provv. 30 ottobre 2013, n. 483, doc. web n. 2851973, relativo ad un impianto di videosorveglianza occultato, ed accessibile da remoto, presso un supermercato).

In molti altri casi, pur essendo riconoscibile agli interessati la presenza di un impianto di videosorveglianza, il trattamento è tuttavia risultato effettuato in violazione della disciplina di settore sui controlli a distanza (richiamata dall'art. 114 del Codice): ciò è accaduto in presenza di telecamere che riprendevano gli ambiti spaziali più vari nei quali l'attività dei lavoratori (oltre che di utenti e clienti) poteva svolgersi: in luoghi di cura (provv. 18 aprile 2013, n. 199, doc. web n. 2476068, con riguardo a riprese effettuate nella sala d'attesa e in corrispondenza degli ingressi a strutture sanitarie), nell'area di vendita di un esercizio commerciale e nell'annesso deposito, ove pure erano presenti postazioni di lavoro (provv. 12 settembre 2013, n. 398, doc. web n. 2705679), o, ancora, all'interno di una sala giochi (provv. 8 maggio 2013, n. 231, doc. web n. 2499485); in corrispondenza degli accessi ad un Archivio di Stato e nei suoi corridoi, nelle sale convegno e studio nonché in alcuni ambienti aperti all'utenza per la consultazione di documenti e la visione dei beni archivistici (provv. 18 aprile 2013, n. 200, doc. web n. 2483269); in tal caso, come in altri (cfr. la decisione relativa all'installazione di sistemi di videosorveglianza in sale giochi richiesta in provvedimenti autorizzatori emessi dalla competente autorità di pubblica sicurezza: cfr. provv. 18 dicembre 2013, n. 587, doc. web n. 2914191), il Garante, pur riconoscendo l'ammissibilità dell'installazione dei predetti sistemi di videosorveglianza, ha comunque ritenuto che le operazioni di trattamento delle immagini raccolte dovessero comunque essere effettuate nel rispetto della disciplina sul controllo a distanza dei lavoratori.

Anche alla luce di accertamenti pregressi, l'Autorità ha poi effettuato controlli a campione nell'ambito della grande distribuzione (cfr. par. 18.4), inserendo tale attività ispettiva tra le proprie priorità. Le verifiche hanno evidenziato ampie aree di inosservanza della disciplina applicabile anzitutto in relazione alla normativa in materia di

controlli a distanza dei lavoratori, con riguardo a telecamere installate, all'esterno e all'interno del punto vendita, in modo da poter riprendere anche l'attività del personale addetto alle casse (provv. 18 luglio 2013, n. 361, doc. web n. 2605290) nonché gli ingressi carrai e pedonali (provv. 4 luglio 2013, n. 334, doc. web n. 2577203) o in ambiti ulteriori nei quali poteva comunque essere rilevata l'attività dei lavoratori (ad es., in un deposito seminterrato: cfr. provv. 4 luglio 2013, n. 335, doc. web n. 2577227; v. pure provv. 30 ottobre 2013, n. 484, doc. web n. 2908871). In qualche occasione sono stati altresì accertati tempi di conservazione delle immagini diversi da quelli previsti dal provvedimento autorizzatorio della competente Direzione provinciale del lavoro e quindi in violazione dei principi di liceità del trattamento (cfr. provv. 5 settembre 2013, n. 385, doc. web n. 2683203).

La mancata designazione di incaricati o responsabili del trattamento come pure l'assenza o l'inidoneità dell'informativa resa agli interessati (finanche secondo le modalità semplificate da tempo fissate dal Garante, da ultimo nel provvedimento generale dell'8 aprile 2010, doc. web n. 1712680) rappresentano due "classici" ulteriori esempi di violazioni riscontrate. Per evitare di incorrere in tali violazioni sarebbe stato sufficiente rendere chiaramente visibili agli interessati appositi avvisi sintetici in grado di rendere gli stessi chiaramente edotti del fatto di accedere all'interno di aree videosorvegliate (provv. 21 novembre 2013, n. 521, doc. web n. 2898732); opportunamente, in particolare in relazione ad esercizi commerciali di ampia estensione (o strutturati su più piani), la collocazione di tali avvisi potrebbe estendersi ad aree ulteriori rispetto al solo accesso agli esercizi commerciali (cfr. provv. 12 settembre 2013, n. 397, doc. web n. 2691507).

In mancanza delle garanzie previste dalla disciplina di settore, il Garante ha ritenuto illecito il trattamento effettuato anche nei casi di produzione da parte del titolare del trattamento (per lo più in tempi successivi all'effettuazione delle verifiche *in loco*) di documentazione volta ad attestare, oltre all'informativa resa ai dipendenti, anche una loro manifestazione di consenso al trattamento posto in essere mediante il sistema di videosorveglianza (provv.ti 4 luglio 2013, n. 336, doc. web n. 2578071; 18 luglio 2013, n. 361, doc. web n. 2605290).

Merita infine richiamare, ancorché già menzionato nella Relazione 2012 (p. 195), il provvedimento con il quale il Garante ha dichiarato illecito un trattamento effettuato tramite un sistema di videosorveglianza (che, tra l'altro, riprendeva anche l'area nella quale era posto l'apparecchio per la rilevazione delle presenze dei lavoratori) installato per finalità antitaccheggio presso un esercizio commerciale di una nota catena distributiva, disponendo (in questo caso) il blocco del trattamento dei dati. Al di là di alcuni (più ricorrenti) profili di illiceità del trattamento rilevati nel caso di specie (da un lato l'inidoneità dell'informativa fornita agli interessati nonché la riscontrata possibilità, dal punto di vista tecnico, di accedere alle immagini registrate con modalità diverse da quelle stabilite nell'accordo con le rappresentanze sindacali, in violazione quindi dei princìpi di liceità e correttezza nel trattamento), il Garante ha ravvisato (anche considerato il consolidato indirizzo interpretativo della giurisprudenza di legittimità: cfr. Cass. pen., sez. III, 3 dicembre 2010, n. 1821) quale ulteriore profilo di illiceità del trattamento la circostanza che il personale incaricato di visionare le immagini per le menzionate finalità antitaccheggio, appartenente a società diversa da quella titolare del trattamento, fosse privo della licenza prefettizia richiesta dalla normativa di settore (art. 134, r.d. 18 giugno 1931, n. 773, Tulps) (provv. 17 gennaio 2013, n. 16, doc. web n. 2291893).

Geolocalizzazione

Con riguardo al fenomeno della geolocalizzazione (in particolare di veicoli) – già oggetto di un provvedimento generale dell'Autorità (provv. 4 ottobre 2011, n. 370, doc. web n. 1850581) – sono stati effettuati approfonditi accertamenti ispettivi a

seguito di una segnalazione nella quale si lamentava, presso un compartimento del gestore della rete stradale nazionale, l'uso improprio (e senza l'adozione delle misure previste in materia di controllo a distanza dei lavoratori) di un sistema informativo denominato *road management tool*, comprendente telecamere e un dispositivo di geolocalizzazione installati su veicoli aziendali. Alla luce delle risultanze emerse, il Garante, pur considerando gli strumenti in questione idonei a concorrere ad una più efficiente gestione del servizio reso (specie in casi di criticità sulla rete stradale), come pure incrementare la sicurezza per i lavoratori (in particolare nel caso in cui gli stessi siano chiamati ad operare in luoghi impervi o in presenza di condizioni ambientali avverse), ha ritenuto che il loro impiego dovesse comunque avvenire nel rispetto dei principi in materia di protezione dei dati personali e della disciplina di settore nonché con modalità concretamente idonee a garantire, in particolare, l'osservanza dei diritti e delle libertà fondamentali, nonché della dignità degli interessati (provv. 7 marzo 2013, n. 103, doc. web n. 2471134). Non è stato invece possibile accertare il lamentato uso improprio di detto sistema a causa di alcune operazioni di modifica dei tempi di conservazione dei dati, effettuate nel corso degli accertamenti ispettivi (e oggetto ora di valutazione da parte della competente autorità giudiziaria), che hanno comportato la cancellazione di tutte le immagini in precedenza registrate nel sistema (il cui termine di conservazione era originariamente decennale).

Solo dopo gli accertamenti, la società ha provveduto, da un lato, a designare incaricati del trattamento soggetti che potevano avere accesso ai dati di localizzazione solo in ragione delle mansioni concretamente svolte e, dall'altro, a concludere, a livello nazionale, un accordo con le rappresentanze sindacali (poi inoltrato ai capi compartimento della società al fine di attivare il confronto con le organizzazioni sindacali locali e condividerne i contenuti tra il personale).

11.2. *Il trattamento di dati biometrici e la rilevazione delle presenze*

Sono continuate a pervenire al Garante segnalazioni (talvolta da parte di direzioni territoriali del lavoro) riferite all'utilizzo di sistemi biometrici (cfr. par. 12.1) finalizzati alla rilevazione delle presenze dei dipendenti. In proposito l'Autorità ha ribadito il proprio consolidato orientamento in base al quale il trattamento di dati biometrici dei lavoratori per finalità di ordinaria gestione del rapporto di lavoro e, in particolare, di commisurazione dell'orario di servizio prestato, non è di regola conforme ai principi di necessità, pertinenza e non eccedenza (cfr. già punto 4 del provv. 23 novembre 2006, linee guida per il trattamento di dati dei dipendenti privati, doc. web n. 1364099 e punto 7 del provv. 14 giugno 2007, linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, doc. web n. 1417809). Indirizzo – condiviso dalla giurisprudenza di merito (Trib. Prato, 19 settembre 2011) e coerente con quanto affermato nel parere 3/2012 sugli sviluppi nelle tecnologie biometriche, adottato il 27 aprile 2012, dal Gruppo Art. 29 – secondo cui "il datore di lavoro è sempre tenuto a cercare i mezzi meno invasivi scegliendo, se possibile, un procedimento non biometrico" – che ammette il trattamento dei dati biometrici solo in casi particolari, di regola per presidiare l'accesso ad "aree sensibili", tenendo conto delle attività che si svolgono nei luoghi presidiati o dei beni nelle stesse custoditi.

Il Garante ha altresì chiarito che si ha trattamento di dati biometrici (diversamente da quanto sovente rappresentato nella documentazione predisposta da società che producono e/o installano sistemi biometrici) – con conseguente applicazione della disciplina in materia di trattamento dei dati personali – anche nel caso in cui il rilievo dat-

tiloscopico, temporaneamente raccolto ai soli fini del completamento della fase di *enrollment*, venga successivamente utilizzato (sotto forma di codice numerico) per le operazioni di verifica e raffronto nell'ambito di procedure di autenticazione.

In termini generali è altresì ricorrente l'inadempimento dell'obbligo di notificare i trattamenti effettuati mediante l'impiego di dispositivi biometrici (cfr. artt. 37 e 163 del Codice) nonché quello di fornire preventivamente ai lavoratori interessati idonei elementi informativi circa le caratteristiche dei trattamenti da effettuarsi (cfr. artt. 13 e 161 del Codice).

Per quanto riguarda la casistica considerata, si segnala l'istanza nella quale un Comune, presso il quale si erano verificati fenomeni di abusi derivanti da un uso improprio del *badge* attribuito ai dipendenti per la rilevazione delle rispettive presenze – peraltro stigmatizzati dall'intervento della magistratura con provvedimenti a carico degli interessati – manifestava l'intenzione di avvalersi per detta finalità di un sistema biometrico. L'Autorità ha in proposito rilevato l'assenza di circostanziati elementi, strettamente rapportati alla specifica realtà lavorativa (quali, ad es., la dislocazione decentrata degli uffici tale da ostacolare un'agevole verifica della corretta esecuzione delle prestazioni lavorative), da cui si potesse effettivamente arguire l'insufficienza di ordinarie misure di controllo (e, correlativamente, la reale indispensabilità del trattamento dei dati biometrici dei lavoratori per la finalità suindicata). Né è risultata comprovata l'adozione da parte dell'amministrazione di sistemi fisici volti ad assicurare la presenza effettiva dei lavoratori durante l'orario di lavoro (ad es., l'installazione dei cc.dd. tornelli) o di ulteriori misure, meno invasive, volte comunque a prevenire il ripetersi di abusi (quali l'associazione di un codice individuale ai *badge* già attribuiti ai dipendenti) o, ancora, l'inefficacia dei controlli ordinari circa la presenza dei lavoratori presso l'amministrazione istante per il tramite dei dirigenti (sui quali anzitutto incombe la verifica quotidiana, peraltro di immediata evidenza, della presenza del personale agli stessi assegnato, il quale, a domanda, può assentarsi dal lavoro solo a seguito di valutazione del superiore gerarchico preposto all'unità organizzativa presso cui presta servizio) ovvero di controlli a campione da parte delle competenti strutture dell'amministrazione comunale non risultando dalle dichiarazioni rese né la frequenza, né le modalità in concreto osservate di utilizzo, in sede di verifica, dei fogli-presenza. Verifiche, queste, di agevole realizzazione, anche considerato il numero contenuto di dipendenti comunali (numero ancor più ridotto ove il fenomeno dell'assenteismo fosse risultato consolidato), delle quali nel caso di specie non è stata dimostrata l'inefficacia e che potrebbero comunque contenere significativamente il rischio di pratiche abusive ove efficacemente contrastate, porendo le stesse configurarsi quali violazioni di carattere penale, oltre che disciplinare e contabile. Peraltro, ad avviso del Garante, il trattamento dei dati biometrici per la finalità considerata, oltre ad essere in linea di principio sproporzionato (come detto), potrebbe in concreto rivelarsi comunque di scarsa utilità nel contrasto dell'assenteismo; tale modalità di rilevazione delle presenze, infatti, non è di per sé in grado di assicurare l'effettiva presenza sul luogo di lavoro dei dipendenti infedeli ove manchino, in pari tempo, efficaci sistemi di controllo e vigilanza sull'effettiva (operosa) presenza dei lavoratori durante l'arco dell'intera giornata lavorativa (specie ove il fenomeno assuma le proporzioni segnalate nel caso in esame) (provv. 31 gennaio 2013, n. 38, doc. web n. 2304669).

L'Autorità ha altresì adottato tre provvedimenti in materia nei confronti di altrettanti istituti scolastici. Nel primo dei casi considerati è risultato essere stato installato (anche a seguito di ispezione effettuata dalla competente Direzione territoriale del lavoro), presso un Liceo scientifico statale, un sistema biometrico (basato sulla rilevazione delle impronte digitali) finalizzato alla rilevazione delle presenze del personale docente. Tale trattamento è stato ritenuto illecito alla luce dei principi di necessità,

pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice) posto che il titolare del trattamento non aveva dato prova dell'esistenza di elementi obiettivi dai quali desumere, rispetto alla legittima finalità di controllo delle presenze, l'inidoneità delle ordinarie misure di controllo. Peraltro l'utilizzo del sistema biometrico è stato ritenuto non conforme alla specifica disciplina dettata per il settore scolastico, in base alla quale l'accertamento delle presenze del personale docente è effettuata mediante la compilazione di apposito foglio firme ovvero del registro di classe (provv. 30 maggio 2013, n. 261, doc. web n. 2502951).

Anche presso un Istituto tecnico industriale è stato installato un sistema biometrico (anch'esso relativo a impronte digitali) allo scopo di controllare le presenze del personale amministrativo, tecnico e ausiliario, stante la dichiarata necessità di prevenire condotte abusive. Anche in questo caso non sono stati rappresentati al Garante elementi concreti riferiti alla specifica realtà lavorativa dell'istituto dai quali poter dedurre l'inefficacia degli ordinari strumenti di controllo della presenza in servizio. Pertanto, pur ribadendo che l'utilizzo dei sistemi biometrici avrebbe potuto risultare legittimo in relazione alla diversa finalità di controllare l'accesso del personale ad aree ove venissero custoditi documenti riservati o attrezzature di valore, l'Autorità ha dichiarato illecito il trattamento dei dati biometrici riferiti ai lavoratori (provv. 30 maggio 2013, n. 262, doc. web n. 2503101).

Alle medesime conclusioni il Garante è pervenuto nel caso di un sistema biometrico di rilevazione delle presenze del personale amministrativo, tecnico e ausiliario installato (come verificato a seguito di accertamenti ispettivi disposti dall'Autorità) presso un Liceo scientifico statale. La scelta di adottare dispositivi basati sulla tecnologia biometrica è stata effettuata in base all'astratta possibilità di utilizzo abusivo degli strumenti tradizionali di controllo delle presenze (ad es., i *badge*), senza peraltro rappresentare l'eventuale effettuazione di controlli circa la presenza in servizio dei lavoratori secondo modalità meno invasive: il trattamento è stato quindi ritenuto illecito alla luce dei già richiamati principi di necessità, pertinenza e non eccedenza (provv. 1° agosto 2013, n. 384, doc. web n. 2578547).

11.3. *L'intermediazione di lavoro e la ricerca e selezione del personale*

Il Garante ha altresì affrontato alcuni aspetti relativi al trattamento di dati personali riferiti a candidati al lavoro. A seguito di una complessa attività istruttoria, nel corso della quale è stato effettuato un accertamento ispettivo, l'Autorità ha verificato che attraverso un sito internet erano stati trattati con modalità ritenute illecite centinaia di migliaia di dati personali (contenuti all'interno di *curricula vitae* e profili) di candidati a posizioni lavorative. Il titolare del trattamento, infatti, è risultato effettuare trattamenti di dati personali dei candidati per finalità di intermediazione tra domanda ed offerta di lavoro, come definita dall'art. 2, comma 1, lett. *b*), d.lgs. 10 settembre 2003, n. 276 (Attuazione delle deleghe in materia di occupazione e mercato del lavoro, di cui alla legge 14 febbraio 2003, n. 30) – in particolare le attività di "raccolta dei *curricula* dei potenziali lavoratori", la "costituzione di relativa banca dati" nonché la "promozione e gestione dell'incontro tra domanda e offerta di lavoro" – senza soddisfare i requisiti previsti dalla legge per lo svolgimento di tale attività soggetta ad autorizzazione (e, tra questi, il conferimento dei dati relativi ai candidati a Cliclavoro, portale del Ministero del lavoro e delle politiche sociali che costituisce la Borsa continua nazionale del lavoro), con conseguente violazione del principio di liceità del trattamento. Sotto diverso profilo, le informazioni conferite dai candidati sono risultate trattate per finalità ulteriori (veicolazione di promozioni per conto del medesimo tito-

lare o di terzi) in assenza di un'informativa chiara e trasparente e senza aver previamente raccolto il libero consenso degli interessati in relazione alle distinte operazioni di trattamento (che dovevano invece formare oggetto di accettazione "in blocco" da parte degli interessati affinché gli stessi potessero utilmente conferire il proprio *curriculum*). Per questi motivi i descritti trattamenti sono stati vietati dal Garante (provv. 5 dicembre 2013, n. 547, doc. web n. 2865637) e copia del provvedimento è stata trasmessa al Ministero del lavoro e delle politiche sociali per i profili di competenza.

In una diversa fattispecie, un'agenzia per il lavoro (regolarmente autorizzata) in occasione dello svolgimento di "colloqui conoscitivi" di candidati a determinate posizioni lavorative acquisiva la copia del documento di identità al dichiarato scopo di riservarsi "un più accurato controllo, in un secondo momento, dell'esattezza dei dati trascritti". Tale attività di acquisizione e conservazione di copia di documenti identificativi già in fase di selezione dei candidati è stata ritenuta dal Garante eccedente (ai sensi dell'art. 11, comma 1, lett. *d*), del Codice) rispetto alla legittima finalità di identificazione dei candidati stessi. Allo scopo deve infatti ritenersi sufficiente l'adozione di misure organizzative volte ad assicurare la corretta identificazione degli interessati – anche previa esibizione di un documento personale – limitando la raccolta delle informazioni a quelle pertinenti e non eccedenti (rilevato che, ad esempio, la carta di identità contiene anche informazioni non rilevanti per il conseguimento delle finalità di preliminare selezione di personale). Pertanto, anche nella prospettiva del contrasto del cd. furto di identità, l'acquisizione di copie di documenti di identità deve limitarsi ai casi previsti da puntuali previsioni normative ovvero qualora ne risulti provata l'indispensabilità (provv. 4 aprile 2013, n. 162, doc. web n. 2484965; v. già provv. 27 ottobre 2005, doc. web n. 1189435).

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

Sempre più frequentemente vengono lamentate forme di accesso ad informazioni personali o di circolazione improprie di dati personali all'interno della realtà lavorativa. In taluni casi, l'accertamento dei trattamenti oggetto di segnalazione è risultato non agevole o impossibile (v., ad es., provv. 1° agosto 2013, n. 383, doc. web n. 2604028, nel quale il Garante, a seguito di una pur articolata istruttoria, in presenza di dichiarazioni non concordanti rese dalle parti del procedimento, ha potuto accertare il solo mancato aggiornamento di dati personali riferiti al segnalante alla luce delle risultanze del libro dei soci; analogamente, nel caso deciso con provv. 8 maggio 2013, n. 232, doc. web n. 2501216, pur non risultando comprovato che note aventi ad oggetto un procedimento disciplinare fossero state trasmesse all'interessato da personale non autorizzato in base alle mansioni attribuite all'interno di un'amministrazione regionale, sulla base degli elementi emersi, il Garante ha comunque prescritto all'ente, quale misura opportuna, di rivalutare le soluzioni organizzative adottate al fine di assicurare maggiore effettività nell'attuazione della disciplina di protezione dei dati personali, con particolare riguardo alla designazione degli incaricati e al coordinamento tra le molteplici unità organizzative presenti all'interno dell'amministrazione).

In molti altri casi sono invece emerse diverse violazioni: così, in una vicenda peculiare, è stata ritenuta illecita la comunicazione effettuata ad una compagnia di assicurazione di dati personali di una lavoratrice al fine di attivare una polizza collettiva da parte del datore di lavoro contraente, in assenza del consenso informato della lavoratrice/assicurata necessario ai sensi degli artt. 13 e 23 del Codice (oltre che in base all'art. 1919 c.c. per i diversi profili contrattuali). Si è ritenuto pertanto (in un contesto di dichiarazioni peraltro discordanti circa l'origine e le modalità di acquisizione dei

dati personali riferiti alla segnalante) di muovere dal contenuto del contratto di assicurazione stipulato dal datore di lavoro che poneva in capo a quest'ultimo (contraente e beneficiario della polizza) l'obbligo di trasmettere all'assicuratore i dati personali riferiti ai propri dipendenti (allo stesso noti) necessari alla predisposizione e alla successiva gestione della polizza collettiva. Nell'ambito del medesimo provvedimento è stata altresì dichiarata l'illiceità del trattamento dei dati riferiti alla segnalante effettuato dalla compagnia di assicurazione in difetto della prescritta informativa (provv. 11 aprile 2013, n. 179, doc. web n. 2492743).

In altra vicenda, il Garante ha ritenuto infondato un reclamo presentato a seguito della comunicazione di informazioni sul reddito di un dipendente (emolumenti percepiti e somme che avrebbero dovuto essere corrisposte all'esito di una transazione in corso) effettuata dal datore di lavoro su richiesta di un legale nell'ambito di un giudizio di separazione personale. Posto che non è necessario acquisire il consenso dell'interessato per effettuare una comunicazione di dati personali quando ciò sia necessario per far valere o difendere un diritto in giudizio (cfr. art. 24, comma 1, lett. *f*), del Codice), le informazioni comunicate sono state ritenute pertinenti e non eccedenti rispetto alla trattazione nel corso della pendente causa di separazione (provv. 11 aprile 2013, n. 180, doc. web n. 2475832).

Anche nel settore del pubblico impiego la materia dell'indebita circolazione di informazioni personali non solo verso l'esterno ma anche all'interno dei contesti lavorativi (verso soggetti non autorizzati), rimane d'attualità. Ciò è confermato dai numerosi casi segnalati, alcuni dei quali aventi ad oggetto dati sensibili dei lavoratori, che evidenziano talora la mancata adozione di idonee procedure interne volte a consentire il corretto trattamento di dati personali (o comunque la loro inosservanza ove previste). Nella maggior parte dei casi, l'Autorità ha accertato l'illiceità delle comunicazioni di dati personali dei lavoratori a soggetti terzi riservandosi di valutare, con separato procedimento, gli estremi per la contestazione delle violazioni amministrative previste dalla disciplina del Codice.

A tale proposito, è stato ribadito che, anche in ambito lavorativo, il trattamento di dati sensibili da parte di soggetti pubblici può essere effettuato in modo lecito solo se previsto da specifica norma di legge ed in relazione ad informazioni ritenute indispensabili per lo svolgimento delle attività istituzionali da parte dell'amministrazione (cfr. artt. 20, comma 1 e 22, comma 3 del Codice). Ciò tanto più se trattasi, come in un caso oggetto di segnalazione, della comunicazione di informazioni su specifiche patologie (nonché sul grado di disabilità conseguito) sofferte dal dipendente di un'azienda sanitaria provinciale avvenuta in occasione della richiesta, avanzata da quest'ultimo, di permanenza in servizio fino al compimento del 67° anno di età. La normativa di settore prevede che, in tale ipotesi, l'amministrazione debba valutare la richiesta in base alle proprie "esigenze organizzative e funzionali", senza riferimento alcuno alla necessità di trattare dati sanitari. Nella vicenda considerata, invece, il dato riferito ad una grave patologia (puntualmente indicata) occorsa al lavoratore ha formato oggetto di menzione nell'ambito di uno scambio di corrispondenza tra diverse articolazioni dell'azienda: ritenuta tale circolazione di informazioni sensibili non indispensabile né pertinente rispetto alla finalità perseguita dall'amministrazione, oltre che lesiva della dignità dell'interessato, il trattamento è stato ritenuto dal Garante illecito; considerato inoltre il contenuto (talvolta anche divergente) delle comunicazioni inviate all'Autorità nel corso dell'istruttoria, il Garante ha altresì prescritto al titolare di rivalutare le soluzioni organizzative esistenti allo scopo di assicurare effettività nell'attuazione della disciplina di protezione dei dati personali, identificando, vista la presenza della figura del "referente aziendale *privacy*", le funzioni competenti ad interloquire con l'autorità di controllo (provv. 18 dicembre 2013, n. 589, doc. web n. 2909040).

Tra le segnalazioni e i reclami pervenuti vale la pena evidenziare quelli relativi alle modalità di notifica di comunicazioni concernenti procedimenti disciplinari ovvero documenti contenenti valutazioni riferite a singoli lavoratori. In particolare, in occasione della consegna al personale di un'autorità portuale delle buste paga nelle quali venivano altresì liquidati gli importi legati al riconoscimento di premi di produttività, era stata consegnata al personale della struttura anche copia di un processo verbale concernente il raggiungimento degli obiettivi oggetto di contrattazione collettiva, contenente altresì le note valutative e la menzione dell'irrogazione di sanzioni disciplinari a carico di una dipendente. Nella vicenda considerata, il Garante ha ritenuto integrata una comunicazione di dati personali in violazione di legge (cfr. artt. 11, comma 1, lett. *a*) e 19, comma 3, del Codice), peraltro avvenuta secondo modalità non conformi al principio di pertinenza e non eccedenza nel trattamento dei dati (art. 11, comma 1, lett. *d*), del Codice). Nel ribadire che il datore di lavoro pubblico, nel legittimo perseguimento della propria attività istituzionale, deve poter tener conto delle eventuali sanzioni disciplinari comminate al personale in sede di commisurazione del premio di risultato (attività che rientra nel novero delle finalità di gestione del rapporto di lavoro), tuttavia, l'Autorità ha precisato che le misure disciplinari adottate non possono essere oggetto di comunicazione a soggetti diversi dall'interessato in assenza di una specifica norma di legge o di regolamento (provv. 3 ottobre 2013, n. 431, doc. web n. 2747867).

Tra le decisioni di analogo contenuto, merita evidenziare due casi concernenti la riconosciuta illiceità, per assenza del presupposto normativo, della trasmissione, da parte di un Tribunale, delle schede valutative relative a due dipendenti ai due diversi enti presso i quali le stesse prestavano temporaneamente la propria attività lavorativa (in un caso per distacco *ex* art. 30, comma 1, d.lgs. 10 settembre 2003, n. 276, in altro per assegnazione temporanea *ex* art. 23-*bis*, comma 7, d.lgs. n. 165/2001).

In entrambe le fattispecie la documentazione contenente dati personali (le menzionate schede di valutazione) era stata trasmessa (in un caso via fax e in un altro mediante casella di posta elettronica certificata) dal personale amministrativo operante presso il Tribunale, indirizzandola, non già alle dirette interessate (come peraltro stabilito dall'accordo sindacale al precipuo fine di consentire alle stesse di formulare le proprie osservazioni), ma ai diversi Uffici presso i quali le due lavoratrici risultavano temporaneamente in servizio, consentendo, per l'effetto, al personale ivi operante di prenderne conoscenza, in carenza di idoneo presupposto normativo (provv.ti 5 dicembre 2013, n. 545, doc. web n. 2894559 e n. 546, doc. web n. 2896275).

La condotta tenuta si è distaccata dalle indicazioni formulate da tempo dal Garante (cfr. le linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico del 14 giugno 2007 e già il punto 5.5 della deliberazione n. 53 del 23 novembre 2006, doc. web n. 1364939, linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati) con le quali si è precisato che "fuori dei casi in cui forme e modalità di divulgazione di dati personali siano regolate specificamente da puntuali previsioni [...], l'amministrazione deve utilizzare forme di comunicazione individualizzate con il lavoratore, adottando le misure più opportune per prevenire la conoscibilità ingiustificata di dati personali [...] da parte di soggetti diversi dal destinatario, ancorché incaricati di talune operazioni di trattamento (ad esempio, inoltrando le comunicazioni in plico chiuso o spillato; invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente; ricorrendo a comunicazioni telematiche individuali)" (punto 5.3). Né la circostanza che possa sussistere in capo al mittente, come nei casi considerati, un legittimo interesse ad acquisire prova dell'avvenuta ricezione

della documentazione inviata, può esonerarlo dall'adottare opportune cautele volte ad evitare che soggetti diversi dal destinatario possano apprenderne il contenuto senza essere a ciò legittimati, prevenendo così lesioni del diritto alla riservatezza e alla protezione dei dati dell'interessato.

Né viene meno l'illiceità della comunicazione per il fatto che il Tribunale, in una delle fattispecie considerate (provv. n. 545/2013, cit.) abbia inviato la documentazione in questione indirizzandola (anziché all'interessata) alla casella di posta elettronica certificata della società presso la quale la medesima prestava servizio. A giudizio del Garante, infatti, il richiamo operato dal titolare del trattamento all'art. 16-*bis*, comma 6, d.l. 29 novembre 2008, n. 185 (convertito con modificazioni, dall'art. 1, l. 28 gennaio 2009, n. 2) non era pertinente, atteso che detta disposizione, nel consentire alle pp.aa. di avvalersi della posta elettronica certificata quale canale comunicativo con i dipendenti della medesima (e di diversa) amministrazione, fa riferimento all'indirizzo di posta elettronica eventualmente ai medesimi assegnato (*uti singuli*) e non, invece, a quello dell'amministrazione presso la quale gli stessi prestano servizio. Ciò si desume dall'art. 47, comma 3, d.lgs. 7 marzo 2005, n. 82 (Cad) che consente alle pp.aa. di utilizzare "per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati", informativa che, peraltro, nel caso di specie, non è risultato sia stata fornita all'interessata. Peraltro, accedendo all'interpretazione fornita dal titolare del trattamento – al di là della circostanza che un novero assai ampio di comunicazioni di natura personale e talora sensibile riferite ai singoli interessati potrebbe essere soggetto ad ampia circolazione nell'ambito delle pp.aa. –, si perverrebbe all'esito opposto voluto dalla norma che mira, come esplicitato dalla rubrica dell'art. 16-*bis*, ad introdurre "misure di semplificazione": semplificazioni che si ottengono consentendo l'invio delle comunicazioni all'indirizzo di posta elettronica assegnato ai dipendenti destinatari delle stesse (non diversamente dai cittadini menzionati all'art. 16-*bis*, comma 5) e non invece obbligando (invero irrazionalmente) le amministrazioni ad utilizzare i propri indirizzi istituzionali di posta elettronica certificata per (poi) far pervenire – secondo canali tradizionali – le comunicazioni ai diretti interessati.

Analogamente, a fronte di un reclamo concernente la comunicazione di dati personali (sensibili) via posta elettronica indirizzata ad una pluralità di destinatari, il Garante ha ritenuto illecita l'operazione di trattamento in ragione delle modalità utilizzate dal datore di lavoro. Nel caso di specie era stata diramata ad alcune stazioni di un corpo forestale e di vigilanza ambientale, all'indirizzo *e-mail* personale di diversi dipendenti e ai superiori gerarchici degli interessati, una comunicazione riguardante 32 dipendenti, cui era allegata una tabella recante i nominativi dei lavoratori che, su richiesta del medico competente, a seguito della visita medica periodica effettuata ai fini dell'accertamento dello stato di salute ed idoneità alle mansioni (ai sensi dell'art. 41, comma 2, lett. *b*), d.lgs. n. 81/2008), avrebbero dovuto sottoporsi ad ulteriori accertamenti sanitari. La tabella riportava altresì per ciascuno il numero di matricola, la data di nascita, il Servizio di appartenenza, nonché l'indicazione delle ulteriori visite ed esami richiesti (provv. 10 ottobre 2013, n. 443, doc. web n. 2774063). La tipologia degli accertamenti medici richiesti per i reclamanti (e per ciascuno degli altri interessati) nell'ambito del procedimento per il rilascio del giudizio di idoneità alla mansione specifica non può, a giudizio del Garante, in assenza di specifica base normativa, essere resa nota a terzi (artt. 11, comma 1, lett. *a*), e 20 comma 1 e 2, del Codice). Sotto diverso profilo, inoltre, gli stessi lavoratori destinatari della comunicazione e convocati per gli accertamenti – rispetto ai

quali, come detto, sarebbe stato opportuno provvedere a comunicazioni individualizzate - non avevano titolo alcuno per venire a conoscenza degli accertamenti clinici disposti in capo ai colleghi, né sussistevano ragioni per mettere i lavoratori reciprocamente a conoscenza anche della specifica natura degli accertamenti prescritti. Con riguardo infine alla comunicazione nei confronti dei superiori gerarchici e delle strutture territoriali del Corpo forestale, l'Autorità ha chiarito che, salve le esigenze di servizio e di gestione dei turni di lavoro, l'avvenuta trasmissione della tabella nominativa è stata effettuata in violazione del principio di indispensabilità, poiché sarebbe stato sufficiente mettere a parte questi ultimi del solo termine fissato per lo svolgimento degli accertamenti del personale di diretta collaborazione al fine di consentire il tempestivo approntamento delle sostituzioni tra il personale, senza indicare la tipologia degli accertamenti sanitari.

Tale orientamento è stato confermato in successive decisioni, tra le quali merita evidenziare la riconosciuta illiceità, per violazione dei principi di necessità, finalità e liceità, del trattamento di dati sensibili concernenti le condizioni di salute di propri dipendenti effettuato da un'azienda sanitaria provinciale. Nel caso considerato, l'azienda aveva inviato nota di solleciro al Comitato di verifica per le cause di servizio relative a dieci dipendenti (e, tra questi, al segnalante), inviando a tutti per conoscenza la medesima nota. Per effetto delle modalità comunicative prescelte, il trattamento dei dati dei dipendenti – legittimamente effettuato dall'Asp limitatamente all'istruttoria del procedimento regolato dal d.P.R. n. 461/2001, con l'adozione delle garanzie ivi previste – è risultato effettuato in violazione degli artt. 11, comma 1, lett. *a*) e 20, commi 1 e 2, del Codice: ciascuno dei dieci interessati, infatti, è stato indebitamente reso edotto dell'esistenza di procedimenti amministrativi riguardanti, oltre che la propria persona, gli altri nove lavoratori e, al contempo, messo a conoscenza di dati concernenti le condizioni di salute di ciascuno di questi (provv. 10 ottobre 2013, n. 442, doc. web n. 2753605). La menzione di procedimenti per il riconoscimento della dipendenza di infermità da causa di servizio facenti capo ai lavoratori contenuta nel sollecito oggetto di segnalazione comporta invero, pur non essendo stata esplicitata nel medesimo la specifica patologia relativa a ciascuno, una comunicazione di dati comunque suscettibile di "rivelare lo stato di salute" degli interessati ai sensi dell'art. 4, comma 1, lett. *d*), del Codice (in merito alla nozione di dato relativo alle condizioni di salute cfr. linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, punto 6.3; provv.ti 27 giugno 2013, n. 315, doc. web n. 2576686; 3 febbraio 2009, doc. web 1597590; 7 luglio 2004, doc. web n. 1068839 e 1068917; v. anche Cass., 1° agosto 2013, n. 18980).

In altra decisione, il Garante ha dichiarato l'illiceità della circolazione avvenuta nell'ambito di un ateneo di documentazione contenente dati relativi alla salute dell'interessata (segnatamente le informazioni relative all'"interdizione dal lavoro" di una docente per le ragioni previste dall'art. 17 comma 2, lett. *a*), d.lgs. n. 151/2001 in presenza di "gravi complicanze della gravidanza o [a] persistenti forme morbose che si presume possano essere aggravate dallo stato di gravidanza"). L'Autorità ha precisato che i dati sensibili in questione, che legittimamente possono essere trattati dalle competenti funzioni e dal personale amministrativo dell'Università a tal fine incaricato del trattamento per la dichiarata finalità di "gestione del rapporto di lavoro" (cfr. artt. 11, comma 1, lett. *a*), 20, comma 1 e 112, comma 1, del Codice), non potevano invece formare legittimamente oggetto di comunicazione a terzi (nel caso di specie ad altro docente nonché ai componenti del Consiglio di Facoltà) non avendo questi titolo alcuno a trattarli per la menzionata finalità di gestione del rapporto di lavoro (provv. 27 giugno 2013, n. 315, doc. web n. 2576686).

11.5. *La pubblicazione* online *di dati personali riferiti ai dipendenti*

In più occasioni (v. anche par. 4.4) il Garante è stato chiamato a pronunciarsi sulla pubblicazione *online*, sui siti istituzionali degli enti pubblici ovvero nell'ambito delle sezioni dedicate all'albo pretorio, di dati, atti o provvedimenti contenenti dati personali (anche sensibili) riferiti a lavoratori o a partecipanti a concorsi e prove selettive.

Occupandosi della lamentata pubblicazione sul sito web di un'azienda per i servizi sanitari di un provvedimento con il quale veniva assunta la determinazione di recedere da un contratto individuale di lavoro, il Garante ha affermato che la determinazione aziendale, suscettibile di pubblicazione in base alla disciplina di settore, era stata tuttavia diffusa sul web nella versione integrale – che riportava, senza alcuna necessità, "in chiaro" l'identità del dipendente –, in violazione dei principi di pertinenza e non eccedenza nel trattamento dei dati personali di cui all'art. 11, comma 1, lett. *d*), del Codice (provv. 1° agosto 2013, n. 382, doc. web n. 2578588; nello stesso senso si è peraltro di recente pronunciata, su una decisione dell'Autorità, Cass. civ., sez. I, 20 luglio 2012, n. 12726 – confermando provv. 9 dicembre 2003, doc. web n. 1054649 – che aveva ritenuto illecita la diffusione da parte di un Comune delle generalità di un proprio dipendente nell'avviso pubblico di convocazione del consiglio comunale nel quale avrebbe formato oggetto di discussione una procedura esecutiva che lo riguardava). Sempre in tale caso, dagli accertamenti effettuati attraverso il motore di ricerca dell'albo aziendale *online* era altresì emerso che, inserendo gli estremi identificativi dell'interessato, una volta rimossa la delibera dal sito, persisteva comunque la possibilità di risalire all'"oggetto" della stessa contenente espressa indicazione del nominativo dell'*ex* dipendente. Pertanto, anche con riguardo a tale secondo profilo, l'Autorità ha dichiarato illecito il trattamento posto in essere dall'azienda e vietato l'ulteriore diffusione delle informazioni riferite all'interessato, atteso che, per il periodo eccedente i 15 giorni previsti dalla disciplina di settore, si era determinata una diffusione illecita di dati personali (artt. 11, comma 1, lett. *a*) e 19 comma 3, del Codice). Come più volte ribadito dal Garante, infatti, trascorsi i periodi di tempo specificatamente individuati dalla disciplina di settore, i dati devono essere rimossi dal web o privati degli elementi identificativi degli interessati (sul punto cfr. par. 5.2, richiamato dal par. 6.B linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web, provv. 2 marzo 2011, n. 88, doc. web n. 1793203).

In altri casi ha formato oggetto di segnalazione la pubblicazione, sui siti web istituzionali di istituti scolastici nonché di altri uffici periferici del Ministero dell'istruzione dell'università e della ricerca, di graduatorie relative al personale docente ovvero al personale amministrativo tecnico ed ausiliario (cd. ATA) contenenti dati personali eccedenti e non pertinenti (quali codice fiscale, domicilio e recapiti telefonici degli interessati): in tali fattispecie, il Garante ha ritenuto illecita la diffusione dei dati eccedenti e non pertinenti rispetto alla finalità di pubblicità delle graduatorie (cfr. provv.ti 6 giugno 2013, n. 275, doc. web n. 2536184; n. 276, doc. web n. 2536409; n. 274, doc. web n. 2535862, in linea con le indicazioni dell'Autorità nelle linee guida del 3 marzo 2011, doc. web n. 1793203). Tale valutazione, peraltro, trova riscontro anche nell'indirizzo recepito dal Ministero dell'istruzione (peraltro interessato della vicenda) – dapprima con circolare del 7 marzo 2008 (prot. 45/dip./segr.) e, da ultimo, del 22 gennaio 2013 (prot. n. AOODGPER510 – Uff. III), diramate alle articolazioni territoriali concernenti la corretta messa a disposizione sul web dei dati personali detenuti dal Sistema informativo centrale del Ministero-SIDI –, anche in considerazione della presenza, all'interno delle citate graduatorie, di dati personali riferiti a un numero elevato di interessati.

In altro caso, concernente la diffusione mediante pubblicazione sul web, a far data dal 2010, di informazioni (segnatamente, l'elenco dei candidati ammessi alla prova scritta, all'esame orale e il diario delle prove), concernenti lo stato di disabilità di un segnalante e di altri partecipanti ad un concorso riservato ai disabili (ai sensi dell'art. 1, l. n. 68/1999, normativa concernente "il diritto al lavoro dei disabili"), l'Autorità, riservandosi di verificare con separato procedimento la sussistenza dei presupposti per le contestazioni delle sanzioni amministrative conseguenti all'illecito trattamento, ha vietato l'ulteriore diffusione su internet dei dati dei soggetti interessati contenuti nelle graduatorie (provv. 6 giugno 2013, n. 277, doc. web n. 2554965). Tanto, in base al divieto di diffusione dei dati idonei a rivelare lo stato di salute (art. 22, comma 8, del Codice) – la cui violazione è stata già stigmatizzata più volte dal Garante (cfr. par. 4.4) – quali le condizioni di invalidità, disabilità o handicap fisici e/o psichici (cfr. provv.ti 22 novembre 2012, doc. web n. 2194472; 29 novembre 2012, doc. web n. 2192671; 7 ottobre 2009, doc. web n. 1664456; 17 settembre 2009, doc. web n. 1658335; 25 giugno 2009, doc. web n. 1640102; 8 maggio 2008, doc. web n. 1521716; 18 gennaio 2007, doc. web n. 1382026; 27 febbraio 2002, doc. web n. 1063639).

12 Le attività economiche

12.1. *Il settore bancario*

Con provvedimento del 28 novembre 2013, n. 533 (doc. web n. 2801010), il Garante è tornato a pronunciarsi sul delicato tema del rapporto tra normativa antiriciclaggio e disciplina di protezione dei dati personali. Traendo spunto da una segnalazione – che aveva evidenziato, nell'ambito delle doverose verifiche effettuate da un ufficio postale ai sensi del d.lgs. n. 231/2007, l'espletamento di controlli su rapporti anche privati intrattenuti dall'interessato con Poste Italiane s.p.a., benché lo stesso operasse nella veste di mero esecutore materiale di un'operazione per conto di un Comune – l'Autorità ha ricordato come i controlli in materia di antiriciclaggio devono essere effettuati rispettando le garanzie previste dalla normativa sulla riservatezza ed essere proporzionati al profilo di rischio del cliente e alle caratteristiche dell'operazione da effettuare. Nel caso esaminato, il segnalante (già conosciuto dalla direttrice dell'ufficio postale) era stato incaricato di effettuare, in rappresentanza del Comune presso cui lavorava, l'acquisto, per poche migliaia di euro, di buoni lavoro da assegnare ad alcuni pensionari; in tale occasione, l'incaricata dell'ufficio postale, anziché limitarsi a identificarlo come semplice esecutore di un'operazione riconducibile all'ente locale, aveva effettuato una verifica nei suoi confronti volta ad analizzare anche i rapporti personali dal medesimo intrattenuti con la società. Nell'accogliere i rilievi formulati dall'istante, il Garante ha ritenuto illecito il trattamento effettuato da Poste Italiane s.p.a., avendo quest'ultima disatteso il principio dell'"approccio basato sul rischio" fissato dalla normativa vigente e svolto verifiche obiettivamente eccedenti e non giustificate dal basso "profilo di rischio" associabile all'interessato e al tipo di operazione richiesta. Il Garante ha quindi prescritto alla società di adottare, al di là del caso di specie, opportune misure formative e tecnico-organizzative in grado di prevenire operazioni di trattamento dei dati personali dei clienti che, nell'ambito dell'espletamento dei doverosi controlli richiesti dalla normativa in materia di antiriciclaggio, non siano conformi al criterio dell'"approccio basato sul rischio" fissato dall'art. 20, d.lgs. n. 231/2007.

A seguito del provvedimento n. 192 adottato dal Garante il 12 maggio 2011 in mareria di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie (in G.U. 3 giugno 2011, n. 127, doc. web n. 1813953) – con il quale l'Autorità ha prescritto adeguate misure volte a impedire accessi indebiti ai dati personali (informazioni bancarie) degli interessati –, è proseguita l'interlocuzione con l'Associazione bancaria italiana (Abi). Quest'ultima, infatti, unitamente a Poste Italiane s.p.a., ha presentato all'Autorità alcuni quesiti in merito all'implementazione delle misure prescritte nel provvedimento nonché una richiesta di differimento del termine per completare l'attuazione delle citate prescrizioni. All'esito dell'attività svolta, il Garante ha adottato il provvedimento n. 357 in data 18 luglio 2013 (doc. web n. 2573636), con il quale, nel rimettere ai titolari del trattamento la valutazione delle soluzioni organizzative più idonee per l'implementazione del sistema, ha fornito i chiarimenti richiesti, in particolare con riferimento all'ambito oggettivo e soggettivo di applicazione del provvedimento precedentemente adottato, accogliendo altresì la richiesta avanzata da Abi di differire l'applicazione del provvedimento, precedentemente fissata al 3 dicembre 2013, al 3 giugno 2014.

Alcune banche hanno presentato richieste di verifica preliminare per avvalersi della rilevazione delle impronte digitali per l'accesso dei clienti alle proprie cassette di sicurezza. Tale sistema avrebbe consentito ai clienti che avessero scelto di utilizzarlo, di potere accedere alle cassette di sicurezza, in modalità *self-service*, 24 ore su 24. La banca avrebbe offerto, quindi, ai propri clienti, due distinte modalità di accesso: quella con il sistema biometrico oppure quella con modalità tradizionali (*smartcard* e *pin*). Nel primo caso, il cliente avrebbe rilasciato l'impronta digitale, appoggiando il dito su un apposito lettore che avrebbe generato "un algoritmo matematico univoco ed irripetibile", memorizzato su una *smartcard* consegnata al cliente con il relativo *pin*, da utilizzare al momento dell'accesso. Non sarebbe stata prevista la conservazione dei dati biometrici raccolti, né da parte della banca, né in archivi centralizzati. Sul solco dei provvedimenti già adottati (cfr. provv. 13 settembre 2012, n. 242, doc. web n. 1927441 e provv. 18 ottobre 2012, n. 298, doc. web n. 2212554 richiamati nella Relazione 2012, p. 199), il Garante ha ribadito la liceità della finalità perseguita e la proporzionalità del trattamento dei dati personali, prescrivendo specifiche misure a garanzia degli interessati (cfr. provv. 14 febbraio 2013, n. 66, doc. web n. 2375735; provv. 19 settembre 2013, n. 106, doc. web n. 2710934). In particolare, oltre all'informativa che deve chiaramente indicare la possibilità per gli interessati di avvalersi del servizio relativo alle cassette di sicurezza con modalità alternative rispetto alla rilevazione dei loro dati biometrici, l'Autorità ha prescritto agli istituti di credito l'adozione di specifici accorgimenti, quali la designazione degli incaricati del trattamento, la conservazione di una descrizione scritta dell'intervento effettuato dall'installatore che attesti anche la conformità del sistema alle disposizioni del disciplinare tecnico (regola n. 25 dell'Allegato B al Codice) nonché la notifica al Garante del trattamento dei dati biometrici prima dell'inizio delle operazioni di trattamento (art. 37, comma 1, *lett. a)*, del Codice).

Sono infine pervenute segnalazioni e reclami concernenti la comunicazione a terzi di informazioni bancarie dei clienti da parte dei dipendenti in assenza del preventivo consenso degli interessati (art. 23 del Codice) e in mancanza di uno dei suoi equipollenti (art. 24). Al riguardo, quando tali comunicazioni sono risultate connesse ad indebiti accessi da parte di dipendenti, si è rinviato a quanto disposto con il citato provvedimento del 12 maggio 2011, precisando che, allo stato, il provvedimento non trova ancora completa attuazione per mancata decorrenza del termine fissato dal Garante per l'implementazione delle misure. A tale proposito, il Garante ha tuttavia ritenuto illecita la comunicazione ad un professionista di dati bancari riferiti ad un correntista (con il quale il primo aveva collaborato in passato e che lo aveva indirizzato presso la banca per richiedere un finanziamento), perché risultato sprovvisto di poteri rappresentativi ed in assenza del preventivo consenso dell'interessato (art. 23 del Codice) nonché di altro requisito equipollente (art. 24), in violazione del principio di liceità e correttezza di cui all'art. 11, comma 1, lett. *a)*, del Codice (cfr. provv. 18 dicembre 2013, n. 588, doc. web n. 2896472). Per tale motivo il Garante ha prescritto alla banca di adottare misure necessarie per assicurare che la comunicazione a terzi dei dati personali di coloro che entrino in contatto con l'istituto avvenga solo con il consenso degli interessati (art. 23 del Codice) o, in difetto, in presenza di uno dei presupposti equipollenti indicati dall'art. 24 del Codice, impartendo, a tal fine, anche adeguate istruzioni ai responsabili e agli incaricati del trattamento.

Infine, con provvedimento del 27 giugno 2013, n. 318 (doc. web n. 2577071), è stato dichiarato illecito il trattamento dei dati personali posto in essere da una banca che, nell'ambito di un procedimento giudiziario presso l'Arbitro bancario e finanziario (Abf), promosso nei suoi confronti da parte di alcuni clienti, non si era limitata a formulare eccezioni di rito o a contestare nel merito le argomentazioni poste dai ricorrenti a fondamento delle proprie pretese, ma aveva riportato fatti riferibili al pro-

curatore delle stesse parti, relative alla risoluzione dell'originario rapporto lavorativo tra la banca e lo stesso procuratore e alla successiva instaurazione di una vertenza dinanzi al giudice del lavoro. Al riguardo, il Garante ha ritenuto tali informazioni eccedenti rispetto alle concrete esigenze difensive della resistente, perché volte non tanto a dimostrare la eventuale scarsa attendibilità delle affermazioni rese dai ricorrenti, quanto a rendere un'immagine negativa, per fatti extraprocessuali e, comunque, estranei alla materia del contendere, del loro procuratore. Ciò ha comportato la violazione dell'art. 11 del comma 1, lett. *a*) e *d*), del Codice, con conseguente inutilizzabilità dei dati stessi (art. 11, comma 2).

Recupero crediti

Viste le numerosissime segnalazioni che sono continuate a pervenire, nonostante la vigenza del provvedimento generale adottato dal Garante il 30 novembre 2005 (doc. web n. 1213644), l'Autorità ha avviato un'attività istruttoria tesa a verificare non solo la liceità del trattamento dei dati personali posto in essere dalle società che svolgono, eventualmente in qualità di "responsabili del trattamento", le concrete attività di recupero crediti, ma anche in che termini le società creditrici, ove titolari, vigilino sull'operato delle predette.

All'esito degli accertamenti, il Garante ha adottato due provvedimenti, con i quali ha inibito l'uso di forme di comunicazione ritenute lesive della dignità dei debitori. Con il primo (cfr. provv. 11 aprile 2013, n. 181, doc. web n. 2497407), il Garante, nel ribadire i principi già affermati con il citato provvedimento del 2005, ha rilevato l'illiceità del comportamento della società incaricata di procedere al recupero del credito, la quale, nel tentativo di contattare la debitrice, aveva interloquito con il figlio e la nuora di costei, rendendoli edotti – in carenza di consenso dell'interessata – dell'esistenza di alcuni ratei di un finanziamento non pagati e del loro complessivo ammontare. Nella medesima fattispecie, il Garante, procedendo ad una attenta valutazione delle concrete attività svolte dall'appaltatore nella gestione del recupero crediti, anche sulla base dei compiti e delle responsabilità previste dallo specifico contratto di servizio, ha altresì riconosciuto che la qualifica di "titolare del trattamento", contrariamente a quanto stabilito nel contratto, poteva essere attribuita solo alla banca creditrice, risultando solo quest'ultima titolare del potere di assumere decisioni sulle finalità e modalità del trattamento svolto dalla società appaltatrice, di impartire istruzioni e direttive vincolanti, nonché di effettuare pregnanti controlli sull'operato della medesima.

Con il secondo provvedimento del 10 ottobre 2013, n. 445 (doc. web n. 2751860), invece, il Garante ha dichiarato illecito il trattamento dei dati personali effettuato a mezzo di "comunicazioni telefoniche preregistrate volte a sollecitare il pagamento", in quanto – come affermato dal provvedimento generale del 2005 – "suscettibile di rendere edotti soggetti diversi dal debitore della sua asserita condizione di inadempimento".

In particolare, l'Autorità, dando seguito ad una segnalazione concernente alcuni solleciti di pagamento preregistrati inviati da una banca, ha ritenuto che il sistema utilizzato non garantisse l'accertamento dell'identità di colui che rispondeva alla chiamata, né desse certezze circa il diritto di costui di venire a conoscenza delle informazioni inerenti la posizione debitoria dell'effettivo interessato. Detto sistema, infatti, limitandosi a rimettere all'interlocutore la sola facoltà di effettuare "una dichiarazione espressa di identificazione", non era idoneo ad assicurare che le informazioni veicolate attraverso le comunicazioni telefoniche preregistrate potessero essere ricevute dall'effettivo avente diritto (debitore o soggetti da costui autorizzati), con conseguente violazione non solo dei principi posti dalla disciplina sulla protezione dei dati personali, ma anche delle specifiche prescrizioni impartite dal Garante con il provvedimento generale del 2005. In tale occasione, comunque, il Garante ha precisato che l'utilizzo, a fini di recupero crediti, di un sistema basato su solleciti di pagamento preregistrati

non integra di per sé un trattamento illecito di dati, potendo essere utilizzato in presenza di idonei accorgimenti tecnici – basati anche su forme di autenticazione – tali da assicurare la ragionevole certezza che la presa di conoscenza delle informazioni oggetto di comunicazione avvenga solranto da parte di chi ne possa essere il legittimo destinatario (il debitore o terzi da lui autorizzati).

12.2. *Il settore assicurativo*

In attuazione del novellaro art. 135, d.lgs. n. 209/2005, il Garante è stato chiamato a rendere un parere (cfr. provv. 10 ottobre 2013, n. 441, doc. web n. 2725053) sullo schema di regolamento predisposto dall'Isrituro per la vigilanza sulle assicurazioni (Ivass) relativamente al funzionamento della "banca dati sinistri" e delle neocostituite "anagrafe testimoni" e "anagrafe danneggiati", funzionali a rendere più efficace la prevenzione e il contrasto alle frodi nel settore delle assicurazioni Rc auto. Al riguardo il Garante, pur condividendo, di massima, l'impostazione del testo sottoposto alla sua attenzione (principalmente orienrara a consentire accessi selettivi alle diverse tipologie di informazioni contenute nel proprio archivio informatico), ha tuttavia formulato alcune raccomandazioni all'Istituto, volte a rendere maggiormente aderenti ai dettami del Codice le adottande disposizioni regolamentari. In particolare, è stato suggerito all'Ivass di circoscrivere l'accesso alla banca dati per le sole finalità di prevenzione e contrasto dei fenomeni fraudolenri nel settore considerato, nonché di cancellare (previo riversamento su altro supporto informatico) i dati identificarivi degli interessati ivi memorizzati decorsi 5 anni dalla data di definizione dei sinistri.

Inoltre, nell'ottica di dare concreta attuazione ai principi di finalità e di trasparenza, il Garante ha raccomandato all'Ivass – benché quest'ultimo non sia a ciò tenuto, in base alle disposizioni vigenti – di dare evidenza dell'esistenza dei menzionati archivi (e dei connessi trattamenti di dari personali) a coloro chc, a vario titolo, possono trovarsi coinvolti in un sinistro, informando sinteticamente gli interessati già in occasione della compilazione del modulo di "Constatazione amichevole di incidente-denuncia di sinistro"; tale soluzione, infatti, potrebbe agevolare la conoscibilità di tali banche dati, accentuandone l'effetto dissuasivo in rapporto a possibili comportamenti fraudolenti.

Infine, con provvedimento del 10 gennaio 2013, n. 5 (doc. web n. 2367235), l'Autorità si è pronunciara sulla liceità della comunicazione a terzi (nel caso di specie, l'ex coniuge della segnalante), da parte di una società assicuratrice, di dati personali (polizza assicurativa e assegno bancario) di un soggetto assicuratò. L'Autorità, accertata l'assenza del consenso dell'interessaro (art. 23 del Codice) e l'inesistenza di un suo equipollente (art. 24 del Codice), ha dichiarato illecito il trattamento, prescrivendo alla società di adottare adeguate misure per sensibilizzare gli incaricati del trattamento all'osservanza delle regole in materia di trattamento dei dati personali e per garantire alla socierà una scrupolosa vigilanza sull'operato di costoro.

12.3. *Autonoleggio ed* event data recorder

A seguito di un'istanza di verifica preliminare formulata ai sensi dell'art. 17 del Codice, l'Autorità è stata nuovamente chiamata a valutare la liceità dei trattamenti connessi all'installazione, a bordo del parco veicoli in dotazione a una società di autonoleggio, di dispositivi satellitari multifunzione annoverabili tra i cd. *event data recorder*. Tali dispositivi, in grado di raccogliere e trasmettere a un apposito centro servizi numerose informazioni relative alle singole vetture (e indirettamente, ai relativi

conducenti), sarebbero stati utilizzati dalla società per garantire alcuni servizi (gestione di eventuali sinistri; ritrovamento di veicoli rubati; assistenza stradale; raccolta dati ed elaborazione statistica; consultazione "storica" degli automezzi; monitoraggio chilometri; diagnostica) solo in parte – secondo quanto sostenuto – comportanti un trattamento di dati personali. All'esito di una complessa istruttoria, l'Autorità ha ammesso i trattamenti oggetto dell'istanza (provv. 7 novembre 2013, n. 499, doc. web n. 2911484), ritenendoli conformi – ove effettuati nel rispetto delle modalità indicate – ai princìpi di liceità, necessità, finalità e proporzionalità (artt. 3 e 11 del Codice); tuttavia, sono state prescritte alla società alcune misure e accorgimenti volti ad assicurare una maggiore tutela degli interessati, sia sul piano dell'informativa da rendere a costoro, sia in relazione all'adozione di ulteriori e più stringenti misure di sicurezza, in grado di garantire l'autenticità, l'accuratezza e l'integrità delle informazioni rilevate dai dispositivi satellitari. L'Autorità ha precisato, inoltre, che i dati trattati per le suddette finalità non potranno essere utilizzati dalla società per profilare i conducenti, né per negare la stipula di nuovi contratti di autonoleggio.

12.4. *La videosorveglianza in ambito privato*

Nel corso dell'anno, il Garante si è pronunciato in relazione a numerose istanze di verifica preliminare (art. 17 del Codice) presentate da alcune società, sia al fine di essere autorizzate a conservare le immagini registrate per tempi superiori alla settimana, sia in vista dell'impiego di sistemi cd. intelligenti.

Con provvedimento del 7 febbraio 2013, n. 40 (doc. web n. 2305006), l'Autorità si è espressa in relazione ad un istanza di verifica preliminare presentata da una società che, operando nel settore dei trasporti e della logistica, si occupa di spedizioni nazionali ed internazionali, compresi i servizi doganali. La richiesta di autorizzazione per il prolungamento dei tempi di conservazione fino a 30 giorni delle immagini registrate presso il magazzino era stata giustificata non solo con l'esigenza di rafforzare il livello di tutela della merce stoccata, ma anche con quella di raggiungere uno *standard* di sicurezza più elevato, in linea con quanto previsto dal sistema di certificazione volontaria sulla qualità e sicurezza dei servizi legati al trasporto della merce, gestito dall'associazione internazionale "*Transported asset protection association*" (TAPA), *standard* di riferimento per gli operatori del settore.

L'Autorità, nel rilevare l'obbligo della società – già titolare della qualifica di "agente regolamentato" e di quella di "operatore economico autorizzato" – ad osservare stringenti norme poste da regolamenti comunitari e, in via amministrativa, dall'Ente nazionale per l'aviazione civile (Enac), ha autorizzato la conservazione delle immagini per il periodo richiesto per consentire l'accertamento, da parte dell'autorità giudiziaria, di eventuali illeciti, rilevando, al contempo, che lo *status* di "operatore economico autorizzato" impone alla società che lo abbia conseguito di comunicare alla dogana eventuali sospetti di reato relativi alle spedizioni trattate e di tenere a disposizione della stessa Autorità le spedizioni su cui si ritenga di dover effettuare dei controlli.

Analoga autorizzazione (provv. 6 giugno 2013, n. 278, doc. web n. 2544109) è stata rilasciata in sede di verifica preliminare ad una società che svolge attività di smistamento, distribuzione, consegna e ritiro pacchi e corrispondenza per conto di società di trasporto allo scopo di conservare per 30 giorni le immagini registrate presso il magazzino; ciò, non solo perché spesso non sarebbe stato possibile risalire con tempestività all'identificazione di un pacco mancante o recante qualche anomalia, ma anche in ragione dell'esigenza di rispondere alle istanze provenienti dagli stessi vettori che, imponendo "una tempistica specifica per la consegna della merce", avreb-

bero reso indispensabile "implementare stringenti misure di sicurezza lungo tutta la filiera al fine di garantire la celerità del servizio" e l'integrità delle spedizioni.

Con il provvedimento del 7 marzo 2013, n. 104 (doc. web n. 2340448), l'Autorità si è pronunciata su una richiesta di verifica preliminare (art. 17 del Codice) di un'azienda produttrice di carta moneta per la realizzazione di banconote, al fine di poter conservare per dodici mesi le immagini acquisite attraverso il sistema di videosorveglianza attualmente in uso. La richiesta è stata fondata sul fatto che la Banca Centrale Europea (BCE), titolare esclusivo del potere di autorizzare l'emissione di banconote in euro all'interno della Comunità, ha imposto ai produttori di banconote euro "accreditati" di conservare, per almeno dodici mesi, le immagini registrate dai sistemi di sorveglianza installati presso i siti produttivi; pertanto, quale "fabbricante" di carta moneta, la società ha dichiarato di essere soggetta alla procedura di "accreditamento di sicurezza" (richiesta dalla BCE) ed al rispetto delle "norme di sicurezza minima per la produzione, l'elaborazione, la custodia e il trasporto delle banconote, delle loro componenti, nonché dei relativi altri materiali e informazioni che necessitano di protezione".

L'Autorità, nel rilevare che la società richiedente, in quanto produttrice di carta per la realizzazione di banconote, è soggetta sia alla disciplina posta dalla decisione del 15 maggio 2008, sia a tutte le ulteriori regole periodicamente emanate dalla BCE – tra le quali quelle di sicurezza minime appositamente emanate nei confronti delle aziende in possesso di accreditamento di sicurezza per la produzione di banconote (cd. *Security rules and procedures for manufacturers of euro secure items*, in vigore dal 2 giugno 2008) che, tra l'altro, impongono che le immagini registrate dagli impianti di videosorveglianza installati presso i siti produttivi vengano conservate "per almeno 12 mesi" (v. art. 10, comma 4) – ha deciso di accogliere la richiesta di allungamento dei tempi di conservazione delle immagini, ritenendola conforme ai principi di non eccedenza e di proporzionalità stabiliti dall'art. 11, comma 1, lett. *d*) ed *e*), del Codice.

Il Garante si è espresso su un'istanza di verifica preliminare (art. 17 del Codice) presentata da una società che opera nel settore dei servizi per l'industria petrolifera *onshore* e *offshore*, in vista dell'installazione di un sistema di videosorveglianza cd. intelligente (perché provvisto di un *software* di "analisi della scena") volto a migliorare il livello di sicurezza del patrimonio aziendale e dei lavoratori presso le proprie sedi. Effettuata un'attenta ricognizione del quadro normativo (d.lgs. 11 aprile 2011, n. 61, attuativo della direttiva 2008/114/CE, che ha individuato nelle infrastrutture del settore energetico una potenziale criticità, anche di rilievo comunitario; decreto del Ministero dell'interno 1° dicembre 2010, n. 269, Allegato D, sez. III, punto 3.b.1, che definisce "obiettivi sensibili" le aziende pubbliche o private del settore energetico) e amministrativo (nota del Prefetto di Milano prot. n. 12b2/09007582 N.C. Div. Gab., all. C) del 15 giugno 2013, che ha rilevato, a fronte di un incremento qualitativo e quantitativo degli eventi pericolosi avvenuti nelle sedi della società, la necessità di dotare il sito produttivo di adeguati sistemi di protezione, comprensivi anche di impianti di videosorveglianza intelligente), ha ritenuto che le infrastrutture delle compagnie operanti nel settore energetico possano costituire concreti obiettivi per azioni di sabotaggio e di terrorismo, ammettendo, quindi, l'attivazione presso i siti della società – e a supporto dei dispositivi di ripresa già esistenti – del sistema di video-analisi oggetto dell'istanza, ritenuto in linea con i principi posti dagli artt. 3 e 11 del Codice (provv. 18 aprile 2013, n. 202, doc. web n. 2475774).

Inoltre, con il provvedimento n. 230 dell'8 maggio 2013 (doc. web n. 2433401), l'Autorità ha affrontato la questione della liceità del trattamento delle immagini dei minori iscritti presso un asilo nido che aveva installato un sistema di videosorveglianza dotato di *webcam*, in grado di consentire ai genitori di controllare i propri

figli durante il periodo di permanenza al nido. L'Autorità, condividendo i principi già affermati dal Gruppo Art. 29 ha ritenuto che l'acquisizione, anche a mezzo *web-cam*, di immagini relative a soggetti in età minore e la loro visione, via web, da parte di terzi muniti di specifiche credenziali di autenticazione, costituiscano operazioni di trattamento di dati personali alle quali deve essere rivolta particolare attenzione. Nel merito, l'Autorità ha ritenuto che le esigenze perseguite dall'asilo nido con l'installazione del sistema (sicurezza delle persone e del patrimonio aziendale; necessità di soddisfare le esigenze rappresentate dai genitori) non fossero sufficienti a ritenere l'installazione della *webcam* necessaria e proporzionata, sottolineando, al contempo, come detto sistema potesse porre in serio pericolo gli interessati, non sussistendo alcuna certezza del fatto che la visione dei genitori fosse limitata ai propri figli e, comunque, che restasse circoscritta ai soli soggetti muniti di credenziali d'accesso al sistema. Pertanto, l'Autorità ha dichiarato illecito il trattamento delle immagini dei minori iscritti presso l'asilo nido, effettuato mediante *webcam* posizionata all'interno dell'area didattica, perché in violazione dei principi di necessità e proporzionalità (artt. 3 e 11, comma 1, lett. *a*) e *d*), del Codice).

Successivamente, con provvedimento del 24 ottobre 2013, n. 467 (doc. web n. 2792798), l'Autorità si è pronunciata su un'istanza di verifica preliminare presentata da una società che opera nel segmento della progettazione e della realizzazione di *card* a banda magnetica e *smartcard* (con *microchip contact* e *contactless*), per il mercato bancario e per i settori *retail*, ID, trasporti e telefonia, curando, in alcuni casi, anche la "personalizzazione" dei supporti. La richiesta di autorizzazione per il prolungamento dei tempi di conservazione fino a 90 giorni delle immagini registrate presso l'azienda è stata giustificata – oltre che con le esigenze di tutela della proprietà aziendale, delle persone e dei dati dei clienti – con la necessità di rispettare i parametri fissati dai circuiti internazionali *MasterCard International* e *Visa International*, che impongono alle società certificate presso di loro l'osservanza di un più elevato *standard* di sicurezza durante l'intero processo di lavorazione.

L'Autorità ha accolto la richiesta – con riferimento alle sole immagini attinenti le aree esterne ai locali, quelle di ingresso e di uscita e le zone ritenute "sensibili" (*caveau*, magazzino, aree di produzione, di ricevimento e di spedizione), e purché la loro utilizzazione avvenisse nel rispetto delle procedure delineate dall'art. 4, l. n. 300/1970 nonché all'esclusivo fine dell'accertamento di eventuali illeciti e dell'individuazione, da parte dell'autorità giudiziaria, dei possibili responsabili –, tenendo conto non solo dell'ubicazione del sito, degli episodi criminosi già verificatisi e dell'estrema delicatezza dell'attività produttiva, comportante l'esigenza di proteggere i dati personali di enormi masse di clienti, ma anche della circostanza che le stesse organizzazioni sindacali si erano espresse favorevolmente, anche in vista dell'indispensabile adeguamento della società alle richieste provenienti dagli stessi enti certificatori.

L'Autorità, infine, si è espressa su una richiesta di verifica preliminare presentata da una società proprietaria di numerose sale da gioco in cui si svolge "attività di raccolta di gioco" a mezzo di apparecchiature videoterminali (VLT) e, contestualmente, di raccolta di denaro per conto dello Stato e/o del Concessionario della rete telematica dell'Amministrazione Autonoma dei Monopoli di Stato (AAMS), allo scopo di conservare per 15 giorni le immagini acquisite attraverso il sistema di videosorveglianza in uso, per salvaguardare il patrimonio aziendale da possibili atti illeciti facilitando l'accertamento di eventuali illeciti commessi da parte delle autorità competenti.

Appurato che la società non avrebbe potuto effettuare il controllo delle monete con cadenze inferiori a 10/15 giorni e, al contempo, che l'esame delle registrazioni per ragioni tecniche ed organizzative non avrebbe potuto concludersi nell'arco di soli sette giorni, l'Autorità ha accolto la richiesta, in quanto conforme ai principi di

necessità, proporzionalità, finalità e correttezza posti dagli artt. 3 e 11 del Codice, precisando che l'accesso alle immagini sarebbe potuto avvenire soltanto in caso di diretta rilevazione di illeciti – con l'osservanza di prestabilite modalità procedurali indicate nei provvedimenti autorizzatori rilasciati ai sensi dell'art. 4, comma 2, l. n. 300/1970 dalle Direzioni territoriali del lavoro competenti – o di richiesta proveniente dalle Forze dell'ordine o dall'autorità giudiziaria (provv. 18 dicembre 2013, n. 587, doc. web n. 2914191).

12.5. *La biometria*

In ragione della proliferazione di sistemi in grado, tra l'altro, di rilevare le caratteristiche dinamiche della firma autografa (ritmo; velocità; pressione; accelerazione; movimento) apposta dai clienti in occasione della sottoscrizione di atti o documenti, l'Autorità è stata chiamata a valutare, nell'ambito di una verifica preliminare presentata da una banca operante solo *online* e per il tramite di promotori finanziari, il trattamento di dati personali e biometrici connesso a un servizio di "firma grafometrica" offerto alla clientela (provv. 12 settembre 2013, n. 396, doc. web n. 2683533). Il sistema, che nell'ottica prospettata integrerebbe i requisiti previsti per la firma elettronica avanzata (d.P.C.M. 22 febbraio 2013), risulterebbe in grado di "sigillare" elettronicamente, all'interno del documento informatico sottoscritto dal cliente, i dati biometrici raccolti dai dispositivi (*tablet*) in dotazione ai promotori, sì da consentire *ex post*, ove richiesto dall'autorità giudiziaria, lo svolgimento di specifiche perizie calligrafiche sulla genuinità della sottoscrizione.

Nel valutare positivamente il trattamento – basato sul libero consenso degli interessati ed effettuato, oltre che nel rispetto dei principi di necessità e proporzionalità, per perseguire finalità lecite rese previamente note agli interessati (artt. 3, 11, 13 e 23 del Codice) –, l'Autorità ha evidenziato che la soluzione proposta (conforme anche agli *standard* ISO) poteva effettivamente contribuire – attraverso la garanzia di autenticità, non ripudio e integrità dei documenti sottoscritti elettronicamente – a conferire maggiore certezza nei rapporti giuridici intercorrenti con gli utenti; nondimeno, ha ritenuto opportuno indicare ulteriori misure a tutela degli interessati, considerato l'impiego "in mobilità" dei dispositivi e la loro possibile utilizzabilità per finalità (e in contesti) ulteriori rispetto a quelli considerati. In particolare, oltre all'adozione di idonee misure volte a ridurre i rischi di alterazione dei dispositivi e di installazione di *software* o applicazioni non autorizzati e potenzialmente pericolosi, è stato prescritto l'impiego di presidi tecnico-organizzativi in grado di assicurare la cancellazione "da remoto" delle informazioni in caso di loro smarrimento o sottrazione. Il Garante ha inoltre sottolineato la necessità che la banca preveda adeguate *policy* per la gestione di eventuali incidenti di sicurezza nell'ambito delle diverse fasi del processo di acquisizione della firma grafometrica.

13 Il trasferimento dei dati all'estero

Con riferimento ai flussi transfrontalieri di dati personali, l'attività del Garante si è caratterizzata sia sul versante delle autorizzazioni ai trasferimenti di dati personali verso Paesi terzi mediante norme vincolanti d'impresa (*Binding corporate rules* - BCR), sia sul piano delle autorizzazioni di carattere generale volte all'attuazione delle decisioni della Commissione europea sull'"adeguatezza" della normativa di protezione dei dati di Paesi non appartenenti all'UE.

In ordine al primo aspetto, è stato confermato il crescente interesse, da parte del settore privato (nella specie, società di carattere multinazionale), per l'utilizzo delle BCR quale strumento per il trasferimento intragruppo di dati personali verso Paesi terzi: relativamente elevato, infatti, è stato il numero di richieste di autorizzazione pervenute nel corso dell'anno (talune delle quali ancora in fase di verifica), il cui esame si è concluso con l'approvazione di sei autorizzazioni, rilasciate al termine di complesse istruttorie.

Nel verificare la conformità con l'ordinamento italiano del resto delle BCR approvato al termine della procedura europea di cooperazione (sulla base della procedura di mutua collaborazione cd. *Declaration on mutual recognition*), l'Autorità ha valutato la rispondenza, anche sul piano fattuale, tra gli impegni assunti dalle società istanti e i criteri stabiliti al riguardo dal Gruppo Art. 29, chiedendo alle stesse maggiori informazioni e, ove necessario, idonee rassicurazioni, soprattutto riguardo alla "clausola del terzo beneficiario", al regime di responsabilità, alla natura e alle finalità delle operazioni di trasferimento poste in essere nonché all'efficacia vincolante delle BCR.

Con riferimento a quest'ultimo aspetto, sono state considerate conformi ai principi sanciti dal Gruppo Art. 29 alcune BCR rese vincolanti attraverso strumenti diversi dal contratto plurilaterale, strumento che, invece, aveva caratterizzato le autorizzazioni rilasciate negli ultimi anni. In particolare, è stato valutato rispondente al requisito dell'efficacia vincolante l'obbligo contrattuale assunto dalle società del gruppo mediante la sottoscrizione di una dichiarazione unilaterale al rispetto delle BCR da parte della capogruppo e di un analogo impegno – contenuto in un apposito documento ("lettera di conferma") – assunto dalla società istante con sede in Italia (cfr. provv. 21 novembre 2013, n. 518, doc. web n. 2830367 e provv. 11 luglio 2013, n. 348, doc. web n. 2635057). Parimenti, è stata considerata idonea, in base al criterio dell'efficacia vincolante, l'impegno sottoscritto da tutte le società facenti parte del gruppo a conformarsi ai principi delle "*policy*" (tra cui anche la "*policy*" BCR) approvate dal consiglio di amministrazione della capogruppo (provv. 30 ottobre 2013, n. 485, doc. web n. 2909094); infine, è stata riconosciuta l'efficacia vincolante dell'impegno assunto in un contratto quadro – sottoscritto da tutte le società del gruppo in qualità di importatori e, al contempo, di esportatori di dati personali, individuante le regole per la stipulazione di successivi contratti aventi ad oggetto il trasferimento transfrontaliero di dati personali – tra le società del gruppo medesimo e contenenti clausole analoghe a quelle dell'accordo quadro (provv. 27 giugno 2013, n. 313, doc. web n. 2576345).

In materia di "clausola di responsabilità" sono stati valutati con particolare attenzione i sistemi di assunzione delle responsabilità in caso di violazione delle BCR diversi da quelli previsti dai documenti del Gruppo Art. 29 ma parimenti idonei ad assicu-

rare una adeguata tutela all'interessato. In particolare, sono stati giudicati positivamente i regimi di ripartizione della responsabilità nei confronti dei singoli esportatori situati in area UE, che consentono all'interessato di rivolgersi, in caso di violazione delle BCR, innanzi alla giurisdizione dello Stato in cui ha sede il soggetto esportatore dei dati (provv. 27 giugno 2013, n. 313 cit.).

In merito alla "clausola del terzo beneficiario", l'Autorità ha posto particolare attenzione sull'esigenza di ottenere, da parte della società istante, idonee rassicurazioni con riguardo alla circostanza che tale clausola, qualora di dubbia formulazione, venga interpretata conformemente a quanto previsto al riguardo dal Gruppo Art. 29 (provv. 20 giugno 2013, n. 302, doc. web n. 2550152); infine, quanto alle caratteristiche dei trasferimenti effettivamente posti in essere, sono state richieste specifiche informazioni volte a precisare l'ambito di applicazione dell'autorizzazione, con puntuale indicazione della tipologia dei dati trasferiti e delle finalità del trasferimento, di regola raggruppate in relazione alle singole categorie di interessati i cui dati sono coinvolti nel trasferimento (provv. 14 marzo 2013, n. 124, doc. web n. 2406306).

Il 2013 si è caratterizzato anche per l'adozione di due autorizzazioni di carattere generale volte a recepire, nell'ordinamento italiano, le decisioni della Commissione europea in merito all'adeguatezza delle normative di protezione dei dati personali della Nuova Zelanda (provv. 14 marzo 2013, n. 123, in G.U. 3 aprile 2013, n. 78, doc. web n. 2343701) e della Repubblica orientale dell'Uruguay (provv. 14 marzo 2013, n. 122 in G.U. 3 aprile 2013, n. 78, doc. web n. 2343793). È stato così ulteriormente ampliato il numero di Paesi non appartenenti all'Unione europea nei confronti dei quali è possibile trasferire dati personali senza l'adempimento di ulteriori formalità (quali quelle previste dagli artt. 43-44 del Codice).

Infine, l'Autorità ha fornito chiarimenti sia con riferimento alle modalità concrete di sottoscrizione delle clausole contrattuali tipo (in particolare, riguardo al nuovo testo adottato dalla Commissione europea n. 2010/87/UE, di recente recepimento da parte del Garante: v. Relazione 2012, p. 208), sia con riferimento all'ambito di applicazione ed alle modalità interpretative delle deroghe previste dall'art. 43 del Codice, in particolare per quanto riguarda il requisito del consenso dell'interessato e quello dell'adempimento di un obbligo di legge.

14 Le libere professioni

14.1. *L'attività forense e investigativa*

Campo di applicazione del Codice

Continuano a manifestarsi gli effetti della novella di cui all'art. 40, comma 2, lett. *a*), d.l. 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla l. 22 dicembre 2011, n. 214, che ha ristretto la nozione di "dato personale" alle informazioni relative esclusivamente a persona fisica (cfr. l'art. 4, comma 1, lett. *b*), del Codice, nel testo attualmente vigente), così escludendo dalla nozione di "interessato" le persone giuridiche. In particolare, la segnalazione di una società che paventava l'illecito e dannoso trattamento di alcuni dati riservati nell'ambito di un giudizio è stata archiviata, in quanto non più riconducibile alla protezione dei dati personali (nota 9 settembre 2013).

Comunicazione di dati a terzi

L'Autorità ha ricevuto una segnalazione con la quale l'interessato ha lamentato l'invio da parte di un avvocato presso il suo indirizzo di lavoro di una lettera concernente questioni personali tra l'interessato e l'assistita dell'avvocato. Il legale ha precisato che la lettera era contenuta in una busta sigillata indirizzata personalmente all'interessato presso l'indirizzo di residenza, e che tale busta era stata a sua volta inserita all'interno del plico inviato all'indirizzo di lavoro dello stesso. L'Autorità ha rilevato che nella vicenda non sono emersi gli estremi di una violazione della disciplina in materia di protezione dei dati personali, in quanto l'avvocato ha adottato opportuni accorgimenti per evitare che la lettera potesse venire a conoscenza di soggetti terzi (nota 12 aprile 2013).

Produzione di documenti in giudizio

Con riferimento alla produzione documentale in sede giudiziaria, il Garante ha confermato che spetta al Giudice adito, ove ritualmente richiesto, la competenza a valutare la liceità del trattamento dei dati personali. Infatti, l'art. 160, comma 6, del Codice stabilisce che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali, ancorché non conforme a disposizioni di legge o di regolamento, restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (note 22 aprile, 23 aprile, 23 ottobre e 30 aprile 2013).

Con riferimento ad una segnalazione relativa al trattamento di dati personali da parte di un avvocato nella fase propedeutica all'istaurazione di un giudizio, il Garanre ha ricordato che il trattamento effettuato per far valere o difendere un diritto in sede giudiziaria non richiede né l'informativa all'interessato (art. 13, comma 5, lett. *b*), del Codice), né il suo consenso (art. 24, comma 1, lett. *f*), del Codice) e che l'esigenza di far valere o difendere un diritto non comporta la necessità che tra le parti interessate sia in corso un procedimento giudiziale. Infatti, il paragrafo 5, punto *b*), del codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive (provv. 6 novembre 2008, doc. web n. 1565171) precisa che il consenso dell'interessato non occorre sia per i dati trattati nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, sia nella fase successiva alla risoluzione giudiziale o stragiudiziale della lite (nota 9 luglio 2013).

Accesso per finalità di difesa a dati detenuti da terzi

L'Autorità ha chiarito la posizione dei soggetti che detengono per legge o per contratto dati personali di terzi rispetto a richieste di accesso presentate da avvocati o investigatori privati per far valere o difendere un diritto dei loro clienti in sede giudiziaria.

In un caso, un avvocato ha rappresentato l'interesse ad ottenere in un giudizio di separazione fra coniugi un certificato del casellario giudiziale relativo al coniuge della sua assistita, ricorrendo una delle ipotesi di cui all'art. 3, l. n. 898/1970. Al riguardo, il Garante ha evidenziato che la disciplina in materia di protezione dei dati personali, pur esonerando dal fornire l'informativa all'interessato e acquisirne il consenso anche chi intende raccogliere "per far valere o difendere un diritto in sede giudiziaria" dati personali detenuti da un altro soggetto, non obbliga il soggetto destinatario dell'istanza a fornire i dati richiesti. Il destinatario della richiesta resta invece tenuto, in qualità di titolare del trattamento, a valutare la liceità di rilasciare informazioni concernenti l'interessato, alla luce della disciplina in materia di protezione dei dati personali e della specifica normativa di settore, costituita nella specie dal d.P.R. n. 313/2002 (nota 11 marzo 2013).

Similmente in un'altra vicenda, un avvocato ha lamentato il riscontro negativo fornito dal gestore di un portale web alla richiesta di conoscere, per la tutela degli interessi del proprio assistito, i dati riguardanti un utente del portale. L'Ufficio ha evidenziato che il trattamento per far valere o difendere un diritto in sede giudiziaria esonera dagli adempimenti relativi all'informativa e al consenso, ma deve essere tenuto distinto dal trattamento consistente nella comunicazione di dati personali, detenuti dal titolare sulla base di disposizioni legislative e/o contrattuali, a chi manifesti la necessità di acquisirli per la suddetta finalità. Il Codice non pone a carico dei titolari del trattamento alcun obbligo a comunicare, ancorché a soggetti qualificati, i dati personali richiesti, costituendo ciò una facoltà, che per essere esercitata deve comunque tener conto delle garanzie che l'ordinamento giuridico appresta agli interessati. In particolare, come già evidenziato dal Garante (cfr. provv. 23 maggio 2001, doc. web n. 39821), il titolare, oltre a valutare l'effettiva necessità della comunicazione ai fini dell'esercizio del diritto di difesa, deve verificare che la natura dei dati, il contesto in cui essi sono trattati e, in particolare, il rapporto giuridico che lega il titolare medesimo all'interessato permetta di esercitare tale facoltà senza violare obblighi nascenti dalla legge o da un rapporto contrattuale (nota 5 settembre 2013).

Accesso ad atti delle pp.aa. per svolgere indagini difensive

Un avvocato ha presentato un'istanza di autorizzazione per il trattamento dei dati sensibili relativi allo stato di salute di una signora, a seguito della condanna in primo grado del suo assistito per reati asseritamente commessi nei confronti della medesima, al fine di far valere, in sede d'appello, la non colpevolezza del proprio assistito. L'Ufficio ha premesso che l'autorizzazione, richiesta dall'art. 26 del Codice, è stata già rilasciata dal Garante con l'autorizzazione generale n. 4/2012 al trattamento dei dati sensibili da parte dei liberi professionisti (doc. web n. 2159250). In particolare, l'autorizzazione stabilisce che il trattamento dei dati sensibili può essere effettuato, tra l'altro, ai fini dello svolgimento da parte del difensore delle investigazioni difensive di cui alla l. 7 dicembre 2000, n. 397 o, comunque, per far valere o difendere un diritto in sede giudiziaria, fermo restando che qualora i dati siano idonei a rivelare lo stato di salute e la vita sessuale, il diritto da far valere o difendere deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile (punto 3). Con riferimento al caso di specie, si è, peraltro, rappresentato che il codice di procedura penale stabilisce che, ai fini delle indagini difensive, il difensore può chiedere i documenti in possesso di una p.a. (nella specie, un'azienda ospedaliera pubblica) e di estrarne copia a sue spese (art. 391-*quater*, commi 1 e 2, c.p.p.). In caso di rifiuto trovano applicazione gli artt. 367 e 368 c.p.p., i quali prevedono uno specifico mezzo di tutela giurisdizionale, nel cui ambito

gli organi giudiziari sono tenuti a valutare la richiesta anche sotto il profilo del rispetto dei principi di protezione dei dati personali, con specifico riferimento all'art. 71 del Codice. L'Ufficio ha dichiarato, pertanto, la propria incompetenza sulla vicenda (nota 29 aprile 2013).

Trattamento per fini esclusivamente personali

Un'interessata ha lamentato una violazione della disciplina in materia di tutela dei dati personali da parte di un avvocato che – nel corso del procedimento disciplinare a suo carico dinanzi a un Consiglio dell'Ordine (rispetto al quale l'interessata assumeva la veste di esponente) – aveva prodotto querele ed esposti presentati da una signora nei confronti dell'interessata, a dire di questa non attinenti all'oggetto del procedimento disciplinare.

L'Autorità, dopo avere osservato che le querele e gli esposti non possono essere considerati dati giudiziari, come definiti dall'art. 4, comma 1, lett. *e*), del Codice, in quanto non costituiscono di per sé dati idonei a rivelare la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p., ha rilevato che il trattamento era stato effettuato dall'avvocato per fini esclusivamente personali, qual è nella specie la propria difesa nel procedimento disciplinare, e che i dati personali oggetto del trattamento non erano stati destinati ad una comunicazione sistematica o alla diffusione (tale non essendo il deposito degli stessi nel procedimento disciplinare). Da ciò deriva che il trattamento in questione non è soggetto all'ambito applicativo del Codice, in conformità a quanto previsto dall'art. 5, comma 3, del Codice medesimo (cfr. par. 16.3). L'Ufficio ha altresì evidenziato che spetta all'organo presso il quale è avvenuto il deposito (nella specie, il Consiglio dell'Ordine degli avvocati) valutare la validità, l'efficacia e l'utilizzabilità degli atti in questione con riferimento al procedimento disciplinare in corso (nota 18 giugno 2013).

Un'interessata ha, altresì, lamentato una violazione del diritto alla tutela dei dati personali dei suoi pazienti da parte di una dottoressa che aveva prodotto in una causa civile degli estratti di alcune cartelle cliniche dell'archivio dell'interessata e un contratto di lavoro subordinato intercorrente tra l'interessata e una propria assistita. Anche in tale caso l'Autorità ha rilevato che il trattamento contestato era stato effettuato dalla professionista per fini esclusivamente personali, qual è nella specie la propria difesa in un procedimento giudiziario, e che i dati non erano stati destinati ad una comunicazione sistematica o alla diffusione, tale non essendo il deposito degli stessi in un procedimento giudiziario. Da ciò è derivato che il trattamento in questione non è soggetto all'ambito applicativo del Codice, in conformità a quanto previsto dall'art. 5, comma 3, del Codice medesimo (nota 18 giugno 2013).

15 Il registro dei trattamenti

Come noto, in attuazione dell'art. 154, comma 1, del Codice, il Garante cura la tenuta *online* del Registro dei trattamenti, formato sulla base delle notificazioni ricevute effettuabili esclusivamente attraverso una procedura telematica – semplificata nei contenuti con provvedimento del 22 ottobre 2008 (doc. web n. 1571196) e rispetto alla quale viene assicurata assistenza sia mediante un servizio di messaggistica automatica, sia grazie al supporto tecnico-amministrativo dell'Ufficio – la cui consultazione – consentita a chiunque e gratuita (art. 37, comma 4, del Codice) – ha luogo attraverso l'accesso ad una sezione del sito web dell'Autorità denominata "servizi *online*". L'obbligo di notificazione al Garante, ossia di comunicare in via preventiva l'intenzione di procedere al trattamento o di modificarne o cessarne uno in corso, sorge in capo al titolare del trattamento dei dati personali ove ricorra uno dei casi previsti dall'art. 37 del Codice e non si versi in una delle ipotesi di esonero individuate dall'Autorità con proprie deliberazioni (v. Relazione 2004, p. 109; provv. 31 marzo 2004, doc. web n. 852561; nota 23 aprile 2004, doc. web n. 993385; nota 26 aprile 2004, doc. web n. 996680; provv. 24 giugno 2011, doc. web n. 1823225).

Nel 2013 gli utenti hanno consultato il Registro con una media giornaliera di oltre 70 accessi e punte superiori ai 200 e, con riguardo al numero delle notificazioni presentate, si rileva un significativo incremento rispetto all'anno precedente; deve altresì segnalarsi l'incremento del numero delle cessazioni (cfr. sez. IV, tab. 1 e 13). Il 57% dei notificanti ha la propria sede nel nord del Paese (cfr. sez. IV, tab. 14).

Quanto all'andamento, nel primo e nel secondo trimestre dell'anno si registra un incremento delle notificazioni rispetto ai corrispondenti trimestri del 2012. Nella seconda metà del 2013 si verifica poi un forte incremento del numero delle notificazioni rispetto ai corrispondenti ultimi due trimestri del 2012, con una tendenza alla crescita che risulta confermata nel mese di gennaio 2014, che ha visto il maggior numero di notificazioni dal 2007 con riguardo al mese di gennaio e, in termini assoluti, è aumentato anche il numero delle cessazioni.

I dati percentuali relativi alla tipologia dei trattamenti notificati nel 2013 confermano nel loro insieme, con alcuni scostamenti, le tendenze del periodo 2004-2012: i trattamenti volti a definire il profilo e la personalità dell'interessato tramite l'ausilio di strumenti elettronici, in incremento (29%); quelli di dati idonei a rivelare lo stato di salute e la vita sessuale (22%) e quelli relativi al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni (19%), coprono da soli il 70% di tutti i trattamenti notificati. Si registra, inoltre, in tale contesto anche una crescita delle notificazioni relative a trattamenti di dati biometrici e una diminuzione di quelle relative a trattamenti di dati genetici (cfr. sez. IV, tab. 15).

Anche nel 2013 le notificazioni presentate direttamente dai titolari hanno superato in numero assoluto quelle presentate tramite intermediario.

Si conferma, infine, come già prospettato lo scorso anno, che la disciplina della materia potrebbe costituire oggetto di modifiche nell'ambito della proposta, presentata dalla Commissione europea il 25 gennaio 2012, di un regolamento generale sulla protezione dei dati personali destinato a sostituire la direttiva 95/46/CE.

Nel testo si ipotizza l'abolizione dell'obbligo per i titolari di notificare i trattamenti di dati personali, sostituito da quello di nominare un *data protection officer* (incaricato della protezione dati, secondo la terminologia della direttiva 95/46/CE) per tutti i soggetti pubblici e per quelli privati al di sopra di un certo numero di dipendenti (per dettagli sull'*iter* delle proposte modifiche v. *infra* par. 19.1).

16 La trattazione dei ricorsi

16.1. *I profili generali*

È difficile riassumere in una sola parola il senso complessivo del lavoro svolto nello scorso anno. Se si guarda al numero complessivo dei ricorsi trattati e all'insieme dei temi affrontati, i termini "assestamento" e "consolidamento" sembrano i più rispondenti alla realtà complessiva. Il numero delle decisioni adottate, duecentoventidue (cfr. sez. IV, tab. 4 e 5), è stato pressoché uguale all'anno precedente e le tipologie principali dei procedimenti instaurati corrispondono grosso modo agli ambiti intorno ai quali da diversi anni si concentrano la maggior parte dei fascicoli in trattazione (e che saranno oggetto di specifico esame nei paragrafi successivi).

Uno sguardo più approfondito (che tenga conto non solo del contenuto immediato delle richieste formulate, ma anche delle ragioni sostanziali che muovono i ricorrenti) permette però di cogliere un filo rosso (a volte curioso, sicuramente sorprendente) che consente di ricondurre molte vicende esaminate alle varie sfaccettature determinate da quel complesso di azioni e reazioni che va sotto il nome (riassuntivo e semplificatorio) di "crisi economica globale". Ne sono testimonianza, prima di tutto, i numerosissimi ricorsi rivolti nei confronti dell'intera galassia degli istituti di credito e delle società finanziarie. In un quadro di persistente crisi economica appare, infatti, di estrema importanza disporre di uno strumento di tutela capace di assicurare (in tempi celeri e con minimo esborso di denaro) la possibilità di ricostruire il quadro completo dei rapporti bancari che fanno capo ad una persona singola o ad un'imprenditore individuale (o alle posizioni riconducibili ad un defunto, grazie alle potenzialità racchiuse nel disposto dell'art. 9, comma 3, del Codice). L'art. 7 del Codice diventa così strumento per ricostruire l'assetto e l'evoluzione di patrimoni e rapporti bancari personali, familiari, imprenditoriali, ed è spesso il punto di partenza per contestare le condizioni contrattuali dei rapporti in essere con il sistema creditizio o, più in dettaglio, per verificare la congruità degli interessi praticati.

Più spesso le potenzialità di acquisizione di dati e informazioni messe a disposizione dal Codice sono lo strumento indispensabile per verificare la liceità del trattamento operato nell'ampio settore della centralizzazione dei rischi di credito e in quello ancora più esteso delle banche dati che forniscono elementi di informazione sulle imprese (e più specificamente sulle persone ad esse preposte), sulla correttezza e tempestività di queste nell'onorare le scadenze dei pagamenti e, più in generale, sulla loro affidabilità economica.

Non è un caso, quindi, che ormai da anni, il Garante sia diventato un punto di riferimento in questa materia grazie agli orientamenti espressi in relazione, in particolare, al settore (assai ampio) che comprende i trattamenti effettuati presso i sistemi di informazioni creditizie, la Centrale dei rischi della Banca d'Italia e la Centrale d'allarme interbancaria.

Se quello descritto è il profilo positivo e fisiologico dell'utilizzo della normativa sulla protezione dei dati personali a tutela delle posizioni degli attori "deboli" del sistema economico, in un momento di crisi economica diffusa, non si può però sottacere che gli stessi strumenti a volte appaiono usati in modo strumentale per finalità prevalentemente dilatorie. Su questo confine, a volte contrassegnato da chiaroscuri, si

deve esercitare il senso di responsabilità dell'Autorità, chiamata a fornire interpretazioni e ad adottare decisioni che salvaguardino le effettive esigenze di tutela degli interessati senza dimenticare però le ragioni delle imprese e le necessità di tutela del sistema bancario e finanziario in genere.

16.2. *Uno sguardo ai dati statistici*

Una conferma di questo panorama generale si desume anche dall'analisi dei dati statistici riferiti al 2013, sia prestando attenzione alla tipologia di decisioni adottate, sia con riguardo alle categorie di titolari del trattamento.

Dal primo punto di vista, si conferma con assoluta evidenza l'alto numero di decisioni di non luogo a provvedere (pari al 60% del totale), cioè di procedimenti conclusisi con il soddisfacimento, nel corso dell'istruttoria, delle richieste degli interessati/ricorrenti (procedimenti spesso imperniati su quelle istanze di accesso a dati e informazioni economico-finanziarie cui sopra si è fatto riferimento) (cfr. sez. IV, tab. 4). Una percentuale così significativa di procedimenti conclusisi celermente e positivamente senza dubbio depone a favore dell'utilità e dell'efficacia dello strumento del ricorso, anche se, di riflesso, segnala ancora la persistenza di ambiti di "resistenza" da parte dei titolari del trattamento o (quantomeno) di non conoscenza dei diritti previsti e tutelati dall'art. 7 del Codice, tenendo conto, peraltro, che l'attivazione del ricorso dinanzi all'Autorità è passaggio necessariamente successivo rispetto alla proposizione di un apposito interpello rivolto previamente al soggetto detentore dei dati.

Sul piano della tipologia delle decisioni va comunque sottolineato un incremento significativo dei casi di accoglimento (totale o parziale) delle richieste dei ricorrenti (cfr. sez. IV, tab. 4). Spesso dietro queste vicende si celano istanze articolate (non esclusivamente imperniate su semplici domande di accesso) che attestano una ormai diffusa conoscenza dell'ampio ventaglio delle situazioni giuridiche soggettive riconosciute dalla disciplina di protezione dei dati personali.

Non meno significativo è lo sguardo alle principali categorie di titolari del trattamento (cfr. sez. IV, tab. 5). Pur nella grande varietà di ambiti (praticamente l'intero spettro immaginabile dei soggetti pubblici e privati) emergono in modo evidente le macro-categorie (banche e società finanziarie, sistemi di informazioni creditizie, altri archivi centralizzati relativi alla verifica della affidabilità delle imprese) che sono già state indicate in apertura di questo paragrafo. E a conferma della "sensibilità" dell'ampia casistica dei trattamenti di dati personali connessi allo svolgimento dell'attività economica, va notato anche il numero significativo di procedimenti attivati nei confronti dei datori di lavoro pubblici e privati (circostanza questa che trova conferma anche dal panorama che si ricava dalle segnalazioni e dai reclami pervenuti in questa materia: cfr. par. 11.4). È una casistica che riflette le difficoltà occupazionali del momento, che evidenzia le dinamiche conflittuali diffuse nelle fabbriche e negli uffici e che pone spesso in luce, rispetto all'utilizzo delle nuove tecnologie, il rapporto complesso fra tutela della riservatezza e della dignità dei singoli e le esigenze dell'impresa.

Non può essere sottaciuto, in conclusione, il persistente flusso, già segnalato lo scorso anno, di ricorsi che vengono tuttora proposti (in veste di "interessati") da società commerciali ed enti vari, non ancora consapevoli che le modifiche normative (intervenute alla fine del 2011) alle nozioni di "interessato" e di "dato personale", contenute nell'art. 4 del Codice privano ormai questi soggetti della possibilità di utilizzare gli strumenti di tutela previsti dal Codice, di cui proprio negli ultimi anni erano state

colte le potenzialità. È un fenomeno che va messo in luce, se non altro per segnalare al legislatore e alle associazioni di categoria, il rischio insito in alcune proposte di modifica normativa che, in nome di una malintesa semplificazione, possono sottrarre ulteriori ambiti della vita economica (*in primis* quelle degli imprenditori individuali) alle tutele specifiche della normativa in materia di protezione dei dati personali, riportando in un'area di opacità i trattamenti di dati personali che interessano le realtà imprenditoriali (specie piccole e medie) rispetto al grado di trasparenza alle stesse assicurato dalla disciplina previgente.

16.3. *I profili procedurali*

La varietà dei temi e dei soggetti implicati nella trattazione dei ricorsi e la stessa "elasticità" di molte delle posizioni giuridiche contemplate dall'art. 7 del Codice ha portato da sempre ad un utilizzo ampio dello strumento del ricorso che, lungi dall'essere solo il rimedio al mancato, positivo esercizio del diritto di accesso, ha finito per costituire spesso una sorta di "cavallo di Troia" per utilizzare i rimedi (e la tempistica) prevista in materia di protezione di dati personali al fine di "esplorare" e influenzare la decisione di profili più propriamente pertinenti ad altri ambiti dell'ordinamento giuridico. In questo senso vanno evidenziate le non poche decisioni che hanno permesso di fare luce su diversi aspetti procedurali (a volte anche inediti) fissando quindi i "paletti" dell'area potenzialmente interessata dall'utilizzo dello strumento ricorso.

Vanno anzitutto ricordate le decisioni che hanno messo in luce alcuni profili rispetto ai quali il legislatore ha espliciteamente escluso la possibilità di utilizzare lo strumento del ricorso. In un caso (provv. 27 giugno 2013, n. 324, doc. web n. 2615218) veniva in gioco l'installazione di un impianto di videosorveglianza a tutela di un'abitazione privata che riprendeva però una zona soggetta al transito dell'interessato/ricorrente: in tale fattispecie va fatto riferimento al significativo disposto dell'art. 5, comma 3, del Codice, secondo cui "il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente Codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione". Ne deriva che situazioni analoghe a quella rappresentata, in cui possono darsi ingerenze nella vita privata di singoli, (non rientrando nell'ambito di applicazione del Codice) non possono (neanche) costituire oggetto di richieste *ex* art. 7, né tantomeno di proposizione di ricorso.

Profilo diverso è quello affrontato nella decisione del 21 febbraio 2013, n. 83 (doc. web n. 2413109) concernente una richiesta di "integrazione" dei dati personali dell'interessato contenuti in un'informativa redatta da ufficiali di polizia giudiziaria e rivolta alla procura della Repubblica. Si tratta di fattispecie che, ai sensi del combinato disposto degli artt. 8, comma 2, lett. *h)* e 53 del Codice, rientra fra i trattamenti svolti da "organi di pubblica sicurezza [...] per finalità di [...] prevenzione, accertamento e repressione dei reati" per i quali non è possibile utilizzare lo strumento di tutela di cui agli artt. 145 e ss. (interpello preventivo e successiva, eventuale, proposizione del ricorso).

L'ampia casistica relativa al 2013 ha messo in luce anche alcune situazioni nelle quali i ricorsi sono stati dichiarati inammissibili in quanto proposti da soggetti non legittimati o rivolti a soggetti che di tale particolare strumento di tutela non possono essere destinatari. È il caso della decisione del 6 giugno 2013, n. 285 (doc. web n. 2603890) con la quale, in riferimento ad una richiesta di accesso a informazioni pertinenti ad una controversia in materia bancaria, l'Autorità ha avuto modo di sottolineare che, ai sensi dell'art. 147 del Codice, il ricorso può essere proposto esclu-

sivamente nei confronti del "rirolare del trattamenro" e non anche del soggerto qualificato formalmente come "responsabile" ai sensi dell'art. 29 del Codice (come avvenuto nel caso di specie).

Interessanre anche la vicenda, decisa il 28 novembre 2013, n. 539 (doc. web n. 2943920) nella quale l'Autorità ha ritenuto inammissibile il ricorso proposto da un curatore (privo però di espressa procura) nell'interesse di un soggetto inabilitato. Ciò, seguendo un ormai consolidato orientamento della Corte di cassazione secondo cui "l'inabilitato può stare in giudizio come attore e come convenuto con l'assistenza del curatore [...] atteso che il curatore ha istituzionalmente solo funzioni di assistenza e di supporto, non di rappresentanza o di sostituzione processuale del suo assistito, cui spettano le manifestazioni di volontà processuale" (Cass. civ., sez. I, n. 5359/1992).

Significative e ricche di spunti procedimenrali sono state anche le diverse pronunce incentrate sull'esercizio del diritto di accesso ai dati riferiti ai defunti (che abbiamo già segnalato come efficace strumento per l'impostazione o la risoluzione di complesse controversie ereditarie). Basti ricordare al riguardo le decisioni del 6 giugno 2013, n. 289 (doc. web n. 2605463) e del 26 settembre 2013, n. 419 (doc. web n. 2745548) che hanno permesso di mettere in luce l'ampia platea dei soggetti che possono avere titolo a richiedere le informazioni riferite al defunto, atteso il disposto dell'art. 9, comma 3, del Codice che legittima "chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione", formula di evidente ampiezza che, in particolare, è svincolata dalla configurazione in capo all'interessato della qualità di erede.

Non si può sottacere che l'utilizzo di questa ampia possibilità di accesso (innestata sulle già segnalate rilevanti potenzialità dell'art. 7 del Codice) ha dato luogo a forme di abuso e a richieste di tipo esplorativo che hanno comportato oneri significativi (si pensi al caso degli istituti di credito). È stata così riaffermata (provv. 21 novembre 2013, n. 525, doc. web n. 2936729) la proposta di superare la tendenziale gratuità dell'esercizio del diritto di accesso, dando attuazione al disposto dell'ultima parte dell'art. 10, comma 8, del Codice. Si tratta di tema delicato, che potrà essere oggetto di approfondimento, cui l'Autorità si è fino ad ora accostata con doverosa prudenza e con riferimento al solo ambito dei sistemi di informazioni creditizie.

16.4. *La casistica più significativa*

Merita ora passare rapidamente in rassegna alcuni degli ambiti più significativi interessati dai ricorsi nel 2013. L'elenco (come detto, parziale) mira a segnalare alcuni provvedimenti che, in ragione della loro valenza generale, possono fornire utili indicazioni ai soggetti interessati ad attivare le tutele di cui all'art. 7 del Codice in relazione ad ambiti analoghi.

Trattamenti presso società fornitrici di servizi telefonici e telematici

Lo sviluppo delle tecnologie e la diffusione di apparecchiature informatiche a tutti i livelli e per tutti i tipi di attività ha ovviamente moltiplicato le possibilità di trattamento dei dati personali e il relativo contenzioso. Va però evidenziato che i ricorsi proposti in questa materia nell'ultimo anno si sono concentrati su un aspetto che in passato era stato più volte all'attenzione del Garante: la possibilità di accedere ai cd. dati di traffico. Le norme di riferimento sono rappresentate, come noto, dagli artt. 123 e 132 del Codice, che prevedono un'articolata tempistica di conservazione di tali dati e delimitano in modo puntuale la possibilità di avervi accesso. La consapevolezza della particolare delicatezza di queste informazioni (tenuto conto delle garanzie che assistono la libertà e segretezza delle comunicazioni) e dei diversi soggetti che possono essere interessati da una medesima comunicazione (abbonati e

utenti chiamati o chiamanti) giustifica una disciplina che è, sul punto, attenta e giustamente restrittiva. Disciplina che però non appare molto conosciuta, come dimostrano diversi ricorsi che sono stati dichiarati infondati in quanto formulati con riferimento a iporesi che si pongono al di fuori dei limiti consentiti dal citato art. 132. A tal proposito, si può ricordare la decisione del 28 febbraio 2013, n. 90 (doc. web n. 2414766) relativa ad una richiesta di dati di traffico telefonico già piuttosto risalenti nel tempo. Nel caso di specie, infatti, la richiesta riguardava informazioni rispetto alle quali era già trascorso il termine massimo di conservazione di ventiquattro mesi e, inoltre, l'istanza non era stata formulata con riferimento alle finalità di accertamento e repressione dei reati. Quest'ultimo, indispensabile elemento sta alla base dell'infondatezza anche del ricorso deciso il 26 settembre 2013, n. 421 (doc. web n. 2746125). In tal caso i dati risultavano ancora conservati dall'operatore telefonico ma, essendo già decorsi i sei mesi previsti per la conservazione dei dati a fini di fatturazione ed essendo la richiesta connessa a profili di tutela contrattuali (o comunque civilistica), si esulava dalle previsioni del citato art. 132.

Va infine ricordata la decisione dell'11 aprile 2013, n. 194 (doc. web n. 2544003) che ha visto il positivo esito di una richiesta di accesso a dati di tipo telematico, necessari all'interessato al fine di chiarire i sospetti relativi all'accesso fraudolento da parte di terzi alla propria casella di posta elettronica.

Trattamenti in ambito bancario e finanziario

Si è già avuto modo di sottolineare come sia questo l'ambito rispetto al quale è pervenuto il maggior numero di ricorsi anche nel 2013. Ciò, considerando, naturalmente, questo settore in una accezione larga che comprende non solo le istanze specificamente rivolte nei confronti degli istituti di credito (con particolare riguardo all'esercizio del diritto di accesso), ma anche tutti i procedimenti rivolti (oltre che nei confronti delle banche) nei riguardi dei soggetti (con funzioni di gestione di banche dati o di controllo sulle stesse) che svolgono il ruolo di titolari del trattamento dei dati conservati in alcuni delicati archivi, sia pubblici, sia privati. Il riferimento, naturalmente, è alla Centrale dei rischi istituita presso la Banca d'Italia, alla Centrale d'allarme interbancaria, ma anche e soprattutto, ai soggetti gestori dei sistemi di informazioni creditizie, cui tuttora si indirizzano numerosi ricorsi in relazione al delicato ambito del "credito al consumo". Si tratta peraltro di micro settori caratterizzati da specifiche normative (primarie e/o secondarie) o disciplinate, come nel caso dei sistemi di informazioni creditizie, da fonti atipiche come i codici di deontologia e buona condotta che stabiliscono le modalità di trattamento e la tempistica di conservazione delle informazioni. Sono questi i parametri di riferimento cui il Garante si richiama nell'esaminare questi ricorsi e nel verificarne la liceità dei relativi trattamenti (cfr. provv. 11 aprile 2013, n. 193, doc. web n. 2542632 e provv. 17 ottobre 2013, n. 465, doc. web n. 2925010).

Al di là dei procedimenti che hanno fatto riferimento alle problematiche interpretative di questo complesso di disposizioni (rispetto ai quali nell'anno trascorso non sono emersi profili innovativi ma sostanzialmente una riproposizione di temi sui quali si sono ormai consolidati gli orientamenti del Garante) vi sono però da segnalare alcuni casi che hanno portato all'attenzione dell'Autorità problematiche diverse, e in parte, nuove. In particolare, la decisione del 17 ottobre 2013, n. 463 (doc. web n. 2914255) ha permesso di affrontare per la prima volta il tema dell'accesso alle informazioni trattate nell'ambito delle operazioni (normalmente effettuate con l'ausilio di appositi programmi informatici) di cd. *credit scoring*, cioè il calcolo matematico che precede e (in misura rilevante) condiziona la possibile concessione di un finanziamento o (come nel caso di specie) il rilascio di una carta di credito. Nel caso in esame, la società emittente la carta (che ne aveva negato l'attivazione all'interessato) nel corso del procedimento ha integrato le proprie comunicazioni e, venendo incontro alle richieste del ricorrente volte a conoscere sulla base di quali specifiche informazioni si

era formulato un giudizio "negativo" nei suoi confronti, ha precisato quali dati avevano concorso al calcolo del *credit scoring*, che, nel caso di specie, era risultato inferiore a quello minimo stabilito dalla società per l'emissione del prodotto richiesto.

Interessanti, su altro versante, sono poi due decisioni (del 14 febbraio 2013, n. 70, doc. web n. 2413087 e del 30 ottobre 2013, n. 493, doc. web n. 2929960) con le quali l'Autorità ha avuto la possibilità di confrontarsi con il tema del cd. furto d'identità (realtà purtroppo in costante espansione, tanto da frenare in modo significativo lo sviluppo delle transazioni *online*). Anche in questo caso si è potuta cogliere l'utilità dell'esercizio del diritto di accesso ai dati personali che ha permesso di ricostruire le informazioni da cui la truffa subita dall'interessato ha avuto inizio, attraverso l'acquisizione dei dati (solo parzialmente corrispondenti al vero) riportati sui documenti d'identità contraffatti della vittima del raggiro.

Trattamenti in ambito giornalistico e archivi *online*

In relazione al giornalismo, l'anno 2013 ha confermato in pieno come ormai la quasi totalità delle vicende sottoposte al vaglio dell'Autorità attenga al giornalismo *online*, o riguardi l'ambito televisivo, o interessi il settore, in rapidissima espansione, degli archivi storici digitali delle testate giornalistiche (accessibili gratuitamente e, in alcuni casi, dotati di una profondità temporale di decenni). Da questo punto di vista è anche largamente cambiata la tipologia di contenzioso che si affronta. Sono sempre meno numerose le vicende che vengono portate all'attenzione dell'Autorità per valutazioni sui "contenuti" delle notizie date (profili peraltro che un'autorità amministrativa, per quanto indipendente come il Garante, ha sempre esaminato con prudenza, considerate le particolari guarentigie costituzionali di cui all'art. 21 Cost.), mentre si moltiplicano le ipotesi in cui il trattamento dei dati e, in particolare, le disposizioni del codice di deontologia e buona condotta del settore giornalistico vengono messe in discussione in relazione alle modalità (sotto il profilo della correttezza e liceità delle stesse) con le quali, grazie alle nuove tecnologie, le notizie vengono acquisite, trattate e diffuse. Se questo è già il nuovo fronte dell'informazione, che supera barriere spazio-temporali e professionali (aprendo una rinnovata stagione al giornalismo d'inchiesta anche attraverso l'irruzione del "*citizen journalism*"), non meno rilevanti sono le problematiche (ormai sottoposte al vaglio del Garante con frequenza pressoché quotidiana) legate alla persistenza sulla rete internet ed alla connessa facile reperibilità (in ragione dell'azione dei motori di ricerca) di notizie, anche molto risalenti nel tempo, che possono contenere informazioni (in alcuni casi molto delicate o comunque quasi sempre negative). Tali notizie, inizialmente giustificate da un corretto esercizio del diritto di cronaca, poi sicuramente legittimate nella loro conservazione da esigenze di memoria storica, finalizzata ad assicurare anzitutto la libertà di informazione nonché di studio e ricerca, non di rado, però, riverberano (per un tempo indefinito) un influsso negativo e spesso condizionante sulla vita e le aspettative future di molte persone (che pur possono essere state protagoniste con un ruolo "negativo" di vicende giudiziarie o di cronaca). In questo senso, già da alcuni anni l'Autorità, con una serie numerosa e rilevante di decisioni, ha indicato (significativamente seguita dalla giurisprudenza) la strada della deindicizzazione dei contenuti contestati come strada maestra per assicurare il giusto contemperamento fra le diverse esigenze (ed i connessi valori) sopra evidenziate e le istanze (pressanti e comprensibili) di tante persone comuni che, riassumendo nel concetto evocativo di "diritto all'oblio", le ansie e le negatività indotte da una "esposizione telematica" continua e incancellabile, hanno spinto l'Autorità ad intervenire su questa materia.

Fra le tante decisioni adottate in materia, si possono segnalare quelle del 24 aprile 2013, n. 224 (doc. web n. 2547890) e del 18 dicembre 2013, nn. 597 e 600 (doc. web nn. 2957134 e 2956995) (cfr. par. 9.5). Se questi esempi riflettono un orientamento ormai consolidato, cui sembra peraltro corrispondere un atteggiamento colla-

borativo sempre più diffuso da parte degli editori, non bisogna trascurare i casi (più complessi e delicati) nei quali l'Autorità, oltre al profilo della persistenza in rete degli articoli ormai inseriti negli archivi storici, ha affrontato il problema della pubblicazione di dati avvenuta in modo illecito, in particolare, in violazione delle disposizioni contenute nel codice deontologico di settore, con riferimento, ad esempio, alla diffusione di informazioni, anche dettagliate, sullo stato di salute di una persona (provv. 12 dicembre 2013, n. 578, doc. web n. 2956950) o con riguardo alla pubblicazione di dati identificativi di minori coinvolti, seppure indirettamente, in gravi fatti di cronaca (provv. 18 dicembre 2013, n. 594, doc. web n. 2957346).

Per quanto non attinente alla materia del giornalismo, va infine segnalata una decisione (provv. 21 novembre 2013, n. 516, doc. web n. 2914227) che è strettamente connessa alla materia della deindicizzazione degli articoli dai motori di ricerca. In quesro caso, oggetto delle richieste dell'interessato non era un "pezzo" giornalistico, bensì un'interrogazione parlamentare contenente dati giudiziari (molto risalenti nel tempo e superati da successivi sviluppi processuali) del ricorrente. Pur trattandosi formalmente di una declaratoria di inammissibilità (in ragione della pertinenza dell'attività in questione con lo svolgimento delle funzioni parlamentari assistite nell'ordinamento da una "indipendenza guarentigiata nei confronti di qualsiasi altro potere"), la vicenda ha coinciso con un ripensamento della Camera dei deputati sulle modalità di trattamento di tali questioni. I competenti organi della Camera hanno, infatti, adottato apposite disposizioni procedurali interne (cfr. Deliberazioni dell'Ufficio di Presidenza n. 46/2013 e n. 53/2013, Procedura in ordine a richieste concernenti dati personali contenuti in atti parlamentari) che, recependo linee interpretative e metodologiche già utilizzate in contesti simili (deindicizzazione di notizie disponibili negli archivi storici *online* delle principali testate giornalistiche), hanno offerto anche a queste particolari fattispecie una tutela effettiva e adeguata.

17 Il contenzioso giurisdizionale

17.1. *Considerazioni generali*

Come riferito nella Relazione 2012, il d.lgs. n. 150/2011 con l'art. 34 ha abrogato l'art. 152 del Codice – con l'eccezione del comma 1 –, dettando all'art. 10 nuove regole procedurali concernenti le controversie in materia di applicazione delle disposizioni del Codice in materia di protezione dei dati personali. In particolare, l'art. 34 ha abrogato anche il comma 7 dell'art. 152, che prevedeva esplicitamente l'obbligo della notifica al Garante dei ricorsi proposti direttamente davanti all'autorità giudiziaria, non coinvolgenti le pronunce dell'Autorità.

Tale abrogazione continua a far sentire i suoi effetti negativi sul numero delle notifiche relative a tale tipologia di giudizi effettuate al Garante, che in alcuni casi l'autorità giudiziaria ha continuato a ritenere necessarie; a fronte dei 170 ricorsi notificati nel 2011 e dei 78 nel 2012, nel 2013 sono stati notificati all'Autorità e da questa trattati 32 ricorsi (cfr. sez. IV, tab. 1).

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

Tale strumento, unitamente alle notifiche dei ricorsi proposti direttamente davanti al giudice che l'autorità giudiziaria riterrà di effettuare, potrà consentire al Garante di continuare ad avere conoscenza sull'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).

17.2. *I profili procedurali*

L'art. 152 devolve tutte le controversie riguardanti l'applicazione del Codice, comprese quelle inerenti ai provvedimenti del Garante, all'autorità giudiziaria ordinaria (comma 1), con ricorso da depositare nella cancelleria del Tribunale del luogo ove ha la residenza il titolare del trattamento (art. 10, comma 2, d.lgs. n. 150/2011).

Una pronuncia ha affrontato il problema dell'individuazione del giudice territorialmente competente nel giudizio di opposizione a provvedimenti dell'Autorità nel caso in cui il titolare del trattamento sia una società avente una pluralità di filiali sul territorio nazionale (si trattava, nel caso di specie, di un importante istituto di credito).

Secondo l'art. 152, comma 2, del Codice, applicabile *ratione temporis* alla fattispecie, "l'azione si propone con ricorso depositato nella cancelleria del Tribunale del luogo ove risiede il titolare del trattamento". Il giudice ha reputato che la disposizione citata fosse intesa a radicare la competenza rispetto al luogo di residenza del titolare

"in concreto": il verbo "risiede" non evocherebbe una localizzazione in senso statico del titolare, ma la localizzazione in senso dinamico del suo concreto operare. Assumerebbe rilievo infatti, dal punto di vista dell'interessato, il luogo in cui il trattamento dei dati è stato concretamente percepito. Tale interpretazione è stata sostenuta anche avuto riguardo alle finalità di tutela della normativa in materia di protezione di dati personali: sarebbe infatti irragionevole costringere l'interessato ad esercitare i propri diritti non già nel luogo in cui gli effetti del trattamento si evidenziano e, quindi rivelano la loro capacità lesiva, bensì nel luogo, potenzialmente molto distante, ove ha sede il titolare del trattamento.

Sulla base di tali premesse, è stato ritenuto corretto incardinare la controversia nel luogo dove si trovava la filiale della banca che effettivamente aveva esercitato il trattamento dei dati della ricorrente, escludendo la competenza del tribunale del luogo ove si trova la sede centrale dell'istituto (Trib. Catania, sez. distaccata di Paternò, sentenza 10 giugno 2013, n. 1139).

La menzionata disposizione del Codice, secondo quanto si accennava, è stata successivamente abrogata e sostituita dall'art. 10, comma 2, d.lgs. n. 150/2011, il quale la riproduce nella sostanza, anche se con diverso tenore testuale: "è competente il tribunale del luogo in cui ha la residenza il titolare del trattamento dei dati". Tale modifica dovrebbe definitivamente deporre a favore della competenza del tribunale del luogo dove si trova la sede legale della società, con l'eccezione del caso in cui una sede decentrata, per le particolari caratteristiche che la contraddistinguono, possa essere considerata come autonoma titolare del trattamento dei dati.

Due decisioni si sono occupate della competenza territoriale nei casi in cui una controversia in materia di protezione di dati personali si inserisca nell'ambito di un rapporto di consumo: l'art. 33, lett. *u*), d.lgs. n. 205/2006 (cd. codice del consumo) stabilisce infatti la competenza del giudice del luogo di residenza o di domicilio elettivo del consumatore (derogabile contrattualmente ma, in tal caso, con presunzione di vessatorietà). Sulla scorta di una decisione della Corte di cassazione (ordinanza 14 ottobre 2009, n. 21814), i giudici hanno affermato che il foro previsto dal d.lgs. n. 206/2005 prevale su quello individuato dal Codice, perché la sopravvenienza del primo ha derogato al secondo (Trib. Chieti, sentenza 30 dicembre 2012, n. 833; Trib. Roma, sentenza 18 giugno 2013, n. 12550). Sotto questo profilo, si rileva che – in applicazione del medesimo criterio cronologico indicato dalla Suprema Corte e confermato nelle due pronunce citate – il successivo intervento da parte del d.lgs. n. 150/2011 potrebbe allora indurre a modificare la soluzione prospettata nel senso della prevalenza del foro indicato dalla normativa in materia di tutela dei dati personali.

In tema di giurisdizione, analogamente a quanto accaduto nel 2012, l'Autorità non ha avuto notizia di ricorsi concernenti il trattamento dei dati personali proposti avanti al giudice amministrativo.

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

17.3. *I profili di merito*

Nel 2013 si sono riperute più decisioni emesse dall'autorità giudiziaria, nell'ambito di giudizi nei quali non erano in discussione provvedimenti adottati dal Garante, con riferimento alla divulgazione di dati personali di natura sensibile da parte di una p.a. e il loro trattamento da parte di alcuni istituti di credito. Le fartispecie oggetto dei giudizi concernevano l'illiceità del riferimento da parte dell'ente pubblico erogatore, nella

causale di accredito dei fondi confluiti nei conti correnti bancari dei ricorrenti, beneficiari di presrazioni indennitarie, al titolo giustificativo costituto dalla l. n. 210/1992 (concernente l'indennizzo a favore dei soggetti danneggiati da complicanze di tipo irreversibile a causa di vaccinazioni obbligatorie, trasfusioni e somministrazione di emoderivati) nonché la detenzione di tale dato da parte delle banche ove erano stati aperti i conti. Gli istanti chiedevano l'inibitoria della divulgazione di dati personali sensibili e il risarcimento dei danni subiti.

La maggioranza di tali pronunce hanno rigettato le domande, avendo l'adito Tribunale di Napoli escluso che l'ente pubblico avesse illecitamente propagato i dati sensibili portandoli a conoscenza di soggetti indeterminati, essendosi invece limitato a trasmetterli attraverso una rete informatica ad accessibilità ristretta ad un unico soggetto, ovvero l'istituto di credito ove era stato aperto il conto, che, essendo stato preventivamente autorizzato sulla base del contratto di conto corrente stipulato dall'interessato, riveste il ruolo, unitamente all'ente pubblico, di titolare del trattamento cui comperono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza. In tali casi, anche nei confronti degli istituti di credito il Tribunale non ha ritenuto dimostrato alcun illecito, essendosi verificato che l'unica condotta della banca denunciata come illecita dai ricorrenti e provata *per tabulas* consisteva nella descrizione, effettuata in esecuzione di un preciso obbligo contrattuale, della causale del bonifico disposto dall'ente erogatore nei certificati di estratto conto inoltrati periodicamente alla medesima persona fisica a cui si riferisce il dato personale (Trib. Napoli, sentenze nn. 6383 e 6384 del 16 maggio 2013; in precedenza, sentenze nn. 12068 e 12098 dell'8 novembre 2012).

Può aggiungersi che in passato una sola pronuncia, emessa nel 2011 ma pervenuta al Garante nel 2013, invece, ha accolto il ricorso, evidenziando una diversità di orientamento giurisprudenziale all'interno della medesima sezione del Tribunale di Napoli. In tale decisione, il giudice, confermando che il riferimento alla l. n. 210/1992, contenuto nella causale di accredito in relazione al pagamento dell'indennizzo previsto dalla stessa legge, integra sicuramente un dato sensibile e che costituisce obbligo di legge che i mandati di pagamento contengano la precisa indicazione dell'oggetto della spesa, ha tuttavia ritenuto che debba applicarsi l'art. 22, comma 6, del Codice, il quale stabilisce che i dati sensibili debbano essere trattati, da parte dei soggetti pubblici, con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendano temporaneamente non intellegibili anche a chi è autorizzato ad accedervi (sentenza 7 giugno 2011, n. 7157).

A sostegno di questo orientamento, il giudice ha citato il provvedimento del Garante che, in un caso analogo, ha chiesto al Ministero dell'economia e delle finanze di individuare una modalità di pagamento più rispettosa della riservatezza dei dati sulla salute degli interessati.

Un'altra pronuncia ha riguardato la richiesta di risarcimento del danno (patrimoniale e non) nei confronti di due società operanti nel campo finanziario da parte della persona titolare di una società operante nel medesimo settore e che aveva svolto la propria attività quale agente delle società convenute, le quali avevano comunicato a soggetti terzi dati di natura giudiziaria relativi alla ricorrente. L'illiceità dei comportamenti posti in essere dalle convenute era stata sancita dal provvedimento del Garante del 2 aprile 2008 (doc. web n. 1519711), a seguito di reclamo dell'attrice. In particolare, il Garante aveva rilevato che le comunicazioni lamentate erano state effettuate in assenza della prevista informativa ed erano eccedenti rispetto alle finalità perseguite. Il giudice, nel valutare la sussistenza dei requisiti per il risarcimento del danno, ha ritenuto che, ai fini della prova dell'*an debeatur*, debba ritenersi vincolante la pronuncia del Garante.

Rispetto al *quantum debeatur*, ha ritenuto che la ricorrente non avesse fornito alcuna prova dei danni patrimoniali e non conseguiti, non potendosi considerare sussistente nella specie un danno in *re ipsa*, in adesione con l'orientamento della Suprema Corte (Trib. Napoli, sentenza 12 febbraio 2013, n. 2036).

17.4. *Le opposizioni ai provvedimenti del Garante*

L'anno 2013 ha registrato una lieve flessione nella proposizione delle opposizioni a provvedimenti dell'Autorità: a fronte dei 73 ricorsi del 2012, nel 2013 sono state proposte sessantasette opposizioni (cfr. sez. IV, tab. 1). Di queste, trentotto si riferiscono a opposizioni a ordinanze ingiunzioni, così registrando un aumento rispetto al 2012, nel quale le impugnazioni di tale natura erano state trentaquattro.

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

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

Al riguardo, va rilevato che, rispetto al 2012, si è manifestata una maggiore tendenza dei giudici a ridurre l'importo delle sanzioni irrogate dall'Autorità.

Tra le opposizioni alle ordinanze ingiunzioni, due decisioni hanno riguardato provvedimenti irroganti sanzioni in relazione a trattamenti di immagini raccolte mediante impianti di videosorveglianza, rispettivamente, in un'area portuale e presso una farmacia. In entrambi i casi le valutazioni dell'Autorità sono state confermate ed i ricorsi rigettati (Trib. Vibo Valentia, sez. distaccata di Tropea, sentenza 6 novembre 2012, n. 227; Trib. Piacenza, sentenza 23 maggio 2013, n. 368).

Anche in un altro caso, inerente l'invio, da parte di una società, di comunicazioni indesiderate di carattere promozionale via fax in assenza di informativa e consenso, è stato integralmente confermato il provvedimento del Garante (Trib. Padova, sentenza 4 aprile 2013, n. 877).

In tema di *e-mail* promozionali, il Tribunale di Milano ha confermato l'ordinanza ingiunzione emanata per sanzionare l'invio di tali comunicazioni senza che fossero stati assolti gli obblighi di legge. L'organo giudicante, peraltro, ha ritenuto di ridurre la sanzione, avuto riguardo alle condizioni soggettive del trasgressore (una società artigianale, operante nei confronti di una platea ristretta di utenti) e, per quanto concerne la condotta contestata, il numero assai contenuto di messaggi elettronici inviati (sentenza 17 giugno 2013, n. 8373).

Il Tribunale di Montepulciano, in analoga fattispecie, confermato il provvedimento ingiuntivo nel merito, ha ridotto l'entità della sanzione irrogata, rilevato che non vi era stata né diffusione, né conservazione dei dati trattati nonché la circostanza che l'interessato era stato messo in condizione di consultare l'informativa dopo la ricezione del messaggio di posta elettronica e di comunicare la volontà di non riceverne ulteriori (sentenza 4 aprile 2013, n. 75).

Anche il Tribunale di Santamaria Capua Vetere ha pienamente condiviso le valutazioni svolte dall'Autorità in un caso di omessa informativa relativamente alla raccolta di dati personali dei contribuenti mediante questionari, nell'ambito del servizio di riscossione dei tributi comunali (sentenza 8 maggio 2013, n. 317).

È stato altresì confermato il provvedimento ingiuntivo a carico di una azienda di trasporti per una raccolta di dati personali tramite un *form online*: il giudice si è inserito nel solco di una pacifica giurisprudenza secondo cui, in tema di sanzioni amministrative, è sufficiente e necessaria la coscienza e la volontà della condotta omissiva, senza che occorra la concreta dimostrazione del dolo o della colpa, giacché la norma pone una presunzione (relativa) di colpevolezza a carico del trasgressore. Si è reputato equo, tuttavia, ridurre la sanzione, attesa la minore gravità della violazione ed avuto riguardo al servizio pubblico svolto dall'azienda (Trib. Verona, sentenza 15 marzo 2013, n. 587).

Il Tribunale di Cosenza ha rigettato il ricorso contro un provvedimento emanato nei confronti di un'azienda ospedaliera, con cui il Garante aveva sanzionato una pluralità di violazioni del Codice. Accogliendo le osservazioni della difesa dell'Autorità, il giudice ha rilevato che il pagamento già effettuato non avesse efficacia estintiva dell'obbligazione perché versato dall'azienda, in luogo dell'obbligato, a norma dell'art. 169, comma 2, del Codice, al fine di estinguere il reato di cui al comma 1 del medesimo articolo (sentenza 22 ottobre 2013, n. 1921).

Anche in un'altra controversia vi è stata integrale conferma della sussistenza degli illeciti sanzionati dal Garante: violazione di un provvedimento dell'Autorità, omessa informativa, mancata acquisizione del consenso, mancato riscontro alle richieste di informazioni ed esibizione di documenti effettuate dal Garante, pluralità di violazioni in relazione a banche dati di particolare rilevanza o dimensioni. Il giudice ha ritenuto di operare una riduzione della sanzione, in ragione delle qualità soggettive del trasgressore, come la mancanza di precedenti specifici e le precarie condizioni economiche in cui versava (Trib. Milano, sentenza 15 ottobre 2013, n. 7555).

In materia di rilevazione di dati biometrici, è stato confermato nel merito il provvedimento del Garante che sanzionava l'omessa notificazione all'Autorità dell'avvenuta installazione, all'ingresso del palazzo di un ente pubblico territoriale, di uno strumento di riconoscimento delle impronte digitali, al fine di disciplinare l'accesso all'edificio medesimo.

Il giudice ha ritenuto di ridurre la sanzione pecuniaria, applicando la diminuente di cui all'art. 164-*bis*, comma 1, del Codice, considerato lo scopo perseguito dal ricorrente, la circostanza che il sistema non avesse mai funzionato secondo le intenzioni e, soprattutto, che il lettore non fosse idoneo ad individuare la posizione geografica delle persone mediante una rete di comunicazione elettronica (Trib. Sanremo, sez. distaccata di Ventimiglia, sentenza 6 maggio 2013, n. 75).

È stata altresì confermata l'ordinanza ingiunzione con la quale veniva sanzionata l'omessa risposta ad una richiesta di informazioni del Garante *ex* art. 157 del Codice. Il giudice adito ha respinto la censura relativa al mancato rispetto del termine di novanta giorni per la notifica della contestazione di violazione amministrativa. In conformità ad una consolidata giurisprudenza di merito e di legittimità, richiamata dalla difesa dell'Autorità, si è ribadito che il *dies a quo* va individuato non già in quello della commissione dell'infrazione, bensì nella data di accertamento della medesima da parte dell'organo procedente: la durata dell'istruttoria, peraltro, va valutata in relazione al caso concreto e sulla base della complessità delle indagini tese a riscontrare la sussistenza dell'infrazione e ad acquisire piena conoscenza della condotta illecita, sì da valutarne l'esatta consistenza agli effetti della formulazione della contestazione. L'entità della sanzione è stata tuttavia ridotta a causa delle condizioni economiche del contravventore (Trib. Milano, sentenza 4 luglio 2013, n. 9510).

Un'altra pronuncia ha confermato l'ordinanza ingiunzione emessa sulla base dell'art. 162, comma 2-*bis*, in relazione all'art. 33 del Codice (misure minime di sicurezza). Il Giudice ha ridotto l'ammontare della sanzione al minimo edittale, considerando l'importo già versato dal trasgressore in sede penale e considerato soprattutto il

successivo adeguamento della società ricorrente alla normativa in materia di protezione dei dati personali (Trib. Cagliari, sentenza 15 maggio 2013, n. 1610).

Il Tribunale di Milano ha pienamente confermato nel merito un provvedimento ingiuntivo con cui il Garante aveva sanzionato il trattamento dei dati personali dopo la revoca del consenso dell'interessato da parte di un'agenzia di viaggi *online* ed il mancato riscontro alla richiesta di informazioni dell'Autorità. Il giudice ha tuttavia deciso di operare una leggera riduzione dell'importo della sanzione, in base ad una differente valutazione sulla gravità della condotta (sentenza 16 aprile 2013, n. 5637).

È stato invece dichiarato inammissibile, per difetto di legittimazione, il ricorso sollevato in proprio da soggetto che aveva ricevuto l'ordinanza ingiunzione quale legale rappresentante di una casa di cura che aveva commesso la violazione di cui all'art. 164 del Codice. Per completezza, peraltro, il giudice ha ritenuto di respingere le censure anche nel merito e di confermare la piena legittimità del provvedimento del Garante (Trib. Torino, sentenza 29 novembre 2012, n. 6973).

Due decisioni hanno parzialmente accolto le opposizioni, revocando una delle due sanzioni che l'Autorità aveva irrogato con unico provvedimento.

In tema di messaggi sms contenenti propaganda elettorale, il Tribunale di Milano ha confermato la sanzione per mancata acquisizione del consenso, aderendo alla interpretazione, prospettata dalla difesa del Garante, secondo cui i dati personali non possono essere utilizzati in assenza di manifestazione di volontà dell'interessato solo perché reperibili nella rete internet, essendo necessario che siano inseriti in pubblici registri, elenchi, atti o documenti che sono sottoposti ad una disciplina di conoscibilità da parte di chiunque. Il giudice ha invece ritenuto che fosse applicabile alla fattispecie quanto statuito nel cd. decalogo elettorale del Garante, che esclude l'obbligo di informativa quando si tratti di materiale propagandistico di dimensione ridotte, annullando la relativa sanzione (sentenza 4 dicembre 2013). Contro tale pronuncia, il Garante ha proposto ricorso per cassazione.

In altra decisione, relativa ad una vicenda di rilevazione di dati biometrici dei dipendenti della soprintendenza locale per i beni architettonici, si è ritenuto che il titolare del trattamento, contrariamente a quanto sostenuto nell'ordinanza ingiunzione, avesse assolto l'obbligo di notificazione del trattamento mediante corrispondenza intercorsa con l'Autorità, poiché all'epoca dell'attivazione del sistema non erano ancora state individuate forme specifiche per adempiere a tale obbligo. Il giudice ha invece confermato la sussistenza della violazione relativa all'omessa informativa, ma ha ridotto l'ammontare della sanzione, in base alla minore gravità della condotta e allo scopo perseguito dal trasgressore (Trib. Napoli, sentenza 4 aprile 2013, n. 4358).

Quattro pronunce hanno invece accolto le opposizioni ad altrettanti provvedimenti ingiuntivi emanati dal Garante che, per l'effetto, sono stati annullati.

Due di esse riguardavano ordinanze ingiunzioni adottate a seguito della violazione dell'obbligo di notificazione al Garante del trattamento di dati sensibili (artt. 37 e ss. del Codice).

Nella prima, il giudice ha ritenuto che l'Ausl ricorrente non fosse tenuta a procedere alla notifica in quanto: il trattamento in questione non aveva carattere sistematico; l'esenzione dall'obbligo, formalmente riferita solo ai medici di famiglia e ai pediatri di libera scelta, era applicabile anche alle aziende sanitarie; la ricorrente non era riuscita ad effettuare la notificazione a causa di problemi tecnici legati al sito internet dell'Autorità (Trib. Piacenza, sentenza n. 108 del 27 marzo 2013). Contro tale decisione, il Garante ha proposto ricorso alla Corte di cassazione.

Nel secondo caso, giudicando sulla opposizione proposta da una casa di cura, si è ritenuto, sulla base dell'art. 37, comma 1, lett. *b*), del Codice, che l'obbligo di notifica del trattamento dei dati sensibili non sia imposto in ogni caso di effettuazione di pre-

stazioni sanitarie, ma solo quando sussista una delle finalità previste dalla norma, non rientrandovi i casi di erogazione dei servizi di diagnosi e cura compresi nell'ordinaria attività sanitaria che non siano indirizzati ai fini indicati (Trib. Pescara, sentenza 2 maggio 2013, n. 673).

In una vicenda concernente una sanzione per inidonea informativa a fronte di impianti di videosorveglianza, l'organo giudicante ha dichiarato, disattendendo la ricostruzione in punto di fatto dell'Autorità, che le misure concretamente adottate dal ricorrente erano effettivamente conformi all'art. 3.1 del provvedimento generale del Garante del 29 aprile 2004 (doc. web n. 1003482), applicabile *ratione temporis* alla fattispecie (Trib. Bari, 23 settembre 2013, n. 2798).

In un'altra vicenda si è statuito che la pubblicazione sul sito internet di un ente pubblico territoriale del nome di un individuo e della causa della sua richiesta di riconoscimento dell'infermità da causa di servizio non comportasse un illecito trattamento di dati, in quanto riconducibile all'esigenza di trasparenza amministrativa, legata all'interesse generale a conoscere del procedimento per l'incidenza dell'eventuale esito favorevole sulle risorse patrimoniali della collettività. Il trattamento, secondo il Tribunale, si è svolto nel rispetto dei principi di necessità e proporzionalità dell'azione amministrativa, atteso anche il generico richiamo ad una tabella contenente una elencazione di numerose patologie, tale da non consentire la sicura identificazione dello stato di salute dell'istante (Trib. di Foggia, sentenza 19 novembre 2013, n. 1638). L'Autorità proporrà ricorso in cassazione avverso tale decisione.

La Corte di cassazione ha, infine, dichiarato inammissibili i ricorsi proposti dall'Autorità e dalla controparte avverso una sentenza del Tribunale di Milano di parziale riforma (sul *quantum debeatur*) di una ordinanza ingiunzione emessa dal Garante per violazione dell'obbligo di informativa, sulla base dell'erronea prospettazione del vizio di motivazione della sentenza impugnata e per il tentativo di sollecitare, di fatto, un nuovo giudizio di merito (VI sez. civ., ordinanza 14 giugno 2013, n. 14938).

In un solo caso, risalente al 2012 ma pervenuto all'Autorità l'anno successivo, invece, l'impugnazione è stata proposta avverso il verbale di contestazione di violazione amministrativa. In sintonia con il consolidato orientamento della Corte di cassazione, richiamato dal Garante, il ricorso è stato dichiarato inammissibile in quanto la contestazione non è autonomamente impugnabile, non essendo idonea a costituire titolo per la riscossione della sanzione (Trib. Sassari, sez. distaccata di Alghero, sentenza 16 ottobre 2012, n. 170).

È giunta a conclusione, con il giudizio della Suprema Corte, una controversia relativa alla raccolta dei dati genetici in assenza di consenso dell'interessato: si trattava, in particolare, di mozziconi di sigaretta utilizzati per lo svolgimento di accertamenti biologici di compatibilità genetica, in vista di una successiva azione di disconoscimento della paternità. Il giudice della nomofilachia ha confermato la sentenza del Tribunale di Roma che aveva respinto il ricorso contro il provvedimento inibitorio del Garante (27 novembre 2008, doc. web n. 1581365). Per risolvere il caso, peraltro, la Corte si è pronunciata per l'assoggettamento dei dati genetici alla più ampia disciplina della *privacy* (con riferimento anche all'autorizzazione generale del Garante *ratione temporis* applicabile) affermando i seguenti principi: 1) i dati genetici sono i dati personali dotati del maggior grado di esclusività; 2) essi non si esauriscono in quelli di natura sanitaria od attinenti alla vita sessuale; 3) i dati genetici possono essere dati sensibili, ma hanno una potenzialità predittiva che ne determina l'ontologica diversità; 4) la collocazione dell'art. 90 del Codice nel titolo V dedicato ai dati sanitari e in un capo *ad hoc* dedicato ai dati genetici rappresenta plasticamente tale peculiarità, in quanto stabilisce in via generale un regime derogatorio rispetto agli altri dari personali anche di carattere sanitario che siano fondati su indagini genetiche; 5) al trattamento dei dati

genetici a carattere non sanitario non si applica l'art. 24, comma 1, lett. *f*), del Codice, disciplinante le ipotesi in cui i dati personali possono, previa autorizzazione del Garante, essere utilizzati senza consenso: rispetto a tale disciplina generale, infatti, l'art. 90 si pone come norma derogatoria; 6) al trattamento dei dati genetici di carattere sanitario può invece applicarsi l'art. 26, comma 4, lett. *c*), del Codice.

Nella vicenda in questione, si è affermato che il trattamento, oltre a non avere alcuna finalità sanitaria, non era neanche astrattamente riconducibile all'esercizio in sede giudiziale di un diritto della personalità di rango quanto meno pari a quello dell'interessato (art. 26, comma 4, lett. *c*), del Codice), in quanto non può essere equiparata una valutazione di opportunità *ante causam* diretta a verificare le probabilità di successo in una futura azione di disconoscimento della paternità con la necessaria utilizzazione di alcuni dati come strumenti indispensabili per ottenere tutela giurisdizionale (Corte di cassazione, I sez. civ. sentenza 13 settembre 2013, n. 21014).

La medesima Corte ha, inoltre, respinto il ricorso proposto avverso una sentenza del Tribunale di Milano che aveva confermato, in sede di giudizio di opposizione, un provvedimento emanato dall'Autorità (5 ottobre 2006, doc. web n. 1357375). La vicenda riguardava l'acquisizione da parte del datore di lavoro (nel caso di specie, un istituto bancario) di alcuni dati inerenti ai conti correnti, alle disposizioni di pagamento, all'acquisizione di titoli da parte di un proprio dipendente onde verificare la possibilità di aprire un procedimento disciplinare e, eventualmente, di far valere i propri diritti nelle competenti sedi giudiziarie. Nella sentenza, ribadito come la disciplina posta a tutela dell'interesse alla riservatezza dei dati sia derogabile quando il relativo trattamento sia esercitato per la difesa di un interesse giuridicamente rilevante e nei limiti in cui ciò sia necessario, si richiama la giurisprudenza di legittimità secondo cui la produzione in giudizio di documenti contenenti dati personali è sempre consentita ove necessaria per esercitare il proprio diritto di difesa, anche in assenza del consenso dell'interessato e quali che siano le modalità con cui è stata acquisita la loro conoscenza (I sez. civile, sentenza 11 luglio 2013, n. 17204).

Una controversia ha avuto ad oggetto il sistema di controllo del traffico internet dei dipendenti durante l'orario di lavoro; mediante un apposito *software*, infatti, una società procedeva a memorizzare l'accesso ai siti svolto da ciascun lavoratore, generando *report* individuali e quotidiani, con conservazione dei dati per un tempo variabile tra i sei mesi ed un anno; memorizzava la posta elettronica dei dipendenti e la rendeva accessibile agli amministratori del sistema informatico; controllava il traffico effettuato tramite la tecnologia VoIP.

Il Tribunale è pervenuto alla conferma del provvedimento inibitorio e prescrittivo del Garante (21 luglio 2011, n. 308, doc. web n. 1829641), tramite una ampia e precisa ricostruzione dell'evoluzione della giurisprudenza in tema di controlli cd. difensivi sull'attività del lavoratore e sul rapporto di essi con le garanzie previste dall'art. 4 dello Statuto dei lavoratori (Trib. Roma, sentenza 4 aprile 2013, n. 1196).

Il Tribunale di Pescara ha confermato il provvedimento con il quale il Garante aveva dichiarato illecito il trattamento dei dati personali effettuato a mezzo del sistema di videosorveglianza installato all'interno di un'azienda, con conseguente inutilizzabilità dei dati trattati, e aveva prescritto la designazione di incaricati o, se del caso, responsabili del relativo trattamento (4 ottobre 2012, n. 267, doc. web n. 2066968). Il giudice di merito si è uniformato alla giurisprudenza della Corte di cassazione, evocata dalla difesa del Garante, secondo cui in materia di videosorveglianza le garanzie procedurali imposte dallo Statuto dei lavoratori e dal Codice non trovano applicazione solo quando i controlli (cd. difensivi) riguardino la tutela di beni estranei al rapporto di lavoro e non siano invece anche volti ad accertare comportamenti riguardanti l'esatto adempimento delle obbligazioni discendenti dal rapporto stesso (sentenza 10 ottobre 2013).

In altra controversia è stato rigettato il ricorso di una società avverso il provvedimento con il quale il Garante aveva dichiarato illecito, e conseguentemente vietato, l'invio di fax promozionali ad operatori turistici o titolari di agenzie di viaggi in assenza di una informativa e di un consenso espresso documentato per iscritto e aveva prescritto le misure necessarie ed opportune per rendere il trattamento conforme alla normativa in materia di protezione di dati personali (21 marzo 2012, n. 113, doc. web n. 1895176). Il giudice ha integralmente accolto la ricostruzione, in fatto e in diritto, che ha condotto all'adozione del provvedimento (Trib. Milano, sentenza 10 aprile 2013, n. 4978).

È stato altresì respinto il ricorso contro un provvedimento di infondatezza dell'Autorità (14 luglio 2011, n. 293, doc. web n. 1835222). In quella circostanza, il Garante aveva ritenuto che non vi fosse stata violazione della normativa in materia di protezione di dati personali da parte di una banca che, ricevuto un reclamo per *mobbing* (da cui sarebbero discesi problemi di salute per la reclamante) nei confronti di uno dei propri dipendenti, ne aveva dato notizia al medesimo dipendente nel corso dello svolgimento degli accertamenti interni di natura disciplinare e fornito copia a fini di tutela nelle sedi competenti. Il Tribunale ha confermato la liceità dell'uso dei dati fatto in attività contenziose e precontenziose, condividendo peraltro la posizione dell'Autorità secondo cui il generico riferimento, fatto dallo stesso interessato, a problemi di salute non costituisca di per sé dato sensibile ai fini della più esigente disciplina codicistica (Trib. Roma, sentenza 26 luglio 2013, n. 10817).

Una vicenda ha riguardato la pubblicazione su un quotidiano nazionale di un documento, formato all'interno di una grande azienda radiotelevisiva, contenente l'organigramma della stessa, nel quale i nomi dei dirigenti erano stampati con colori diversi a seconda della loro presunta affiliazione partitica: nell'articolo di commento, inoltre, si denunciava l'occupazione e la lottizzazione della società da parte dei partiti politici. Il Garante, adito separatamente da alcuni dirigenti e dall'azienda stessa, aveva adottato, per quanto qui interessa, provvedimenti di infondatezza (rispettivamente, 30 ottobre 2008 e 12 febbraio 2009, doc. web nn. 1571719 e 1598380). Il Tribunale di Roma, in sede di opposizione ad entrambi i provvedimenti, si è pronunciato sulla vicenda con due distinte sentenze di analogo tenore. Accogliendo le argomentazioni del Garante, il giudice, dopo aver ben distinto gli eventuali profili di rilevanza penale da quelli attinenti alla protezione dei dati personali, ha sottolineato come il trattamento dei dati nell'esercizio di attività giornalistica possa prescindere dal consenso dell'interessato e dall'autorizzazione del Garante, avendo ritenuto il legislatore di dover fornire, quando l'informazione sia essenziale rispetto a fatti di interesse pubblico, una sorta di attenuazione del grado di tutela del diritto alla protezione dei dati personali. Si è ritenuta dunque la pubblicazione non eccedente le finalità del trattamento ma, al contrario, del tutto pertinente ed indispensabile per sostenere il ragionamento seguito (Trib. Roma, sentenze 3 aprile 2013, nn. 13269 e 13268).

Il medesimo ufficio giudiziario, inoltre, ha confermato un provvedimento di non luogo a provvedere del Garante (10 novembre 2010, doc. web n. 1776249): in relazione a delle intercettazioni telefoniche a carico di un dirigente di una società, disposte dall'autorità giudiziaria ed inviate al datore di lavoro per eventuali valutazioni disciplinari, un terzo non destinatario di tale procedimento, che vi compariva in quanto interlocutore, lamentava – a seguito della trasmissione delle intercettazioni al consiglio d'amministrazione dell'azienda – l'indebito trattamento dei propri dati personali. Il giudice ha confermato le valutazioni dell'Autorità, secondo cui non vi erano i presupposti per aprire un autonomo procedimento volto a verificare la sussistenza di eventuali profili di illiceità. Premessa la liceità dell'utilizzo delle intercettazioni telefoniche a fini disciplinari, il Tribunale ha affermato l'inscindibilità del contenuto dell'intercet-

tazione, che coinvolge necessariamente anche un soggetto diverso dal diretto destinatario dell'azione, la cui posizione non può essere separata od oscurata se non a pena di rendere incomprensibile il significato della conversazione. L'interessato, peraltro, aveva ricevuto adeguati ragguagli sul trattamento, essendo egli stesso membro del Cda (Trib. Roma, sentenza 10 luglio 2013, n. 15198).

Una pronuncia, di cui si è già dato conto nel paragrafo riguardante i profili procedurali (cfr. *supra*, par. 17.2), ha confermato il provvedimento (20 settembre 2012, n. 259, doc. web n. 2106524) con cui l'Autorità ha dichiarato il non luogo a provvedere, alla luce dell'esaustivo riscontro inviato dal titolare del trattamento. Il giudice ha inoltre evidenziato, come correttamente il Garante avesse distinto ai fini della propria decisione, la richiesta di comunicazione dei dati personali di cui agli artt. 7 e ss. del Codice e diritto di accesso a documenti bancari previsto dall'art. 119 del Testo unico bancario, diversi nella disciplina e nelle finalità (Trib. di Catania, sez. distaccata di Paternò, sentenza 10 giugno 2013, n. 1139).

È stata dichiarata improcedibile una opposizione avverso un provvedimento di inammissibilità del Garante (4 novembre 2010, doc. web n. 1774912), per la non corretta instaurazione del contraddittorio, ed esattamente per mancato rispetto, da parte del ricorrente, del termine perentorio per la notificazione stabilito dal giudice istruttore a norma dell'art. 152, comma 7, del Codice (successivamente abrogato). Il Tribunale adito non si è pertanto pronunciato sul merito del provvedimento opposto (Trib. Perugia, sentenza 22 febbraio 2013, n. 139).

Una pronuncia si è occupata del tema delle cd. telefonate mute nell'ambito dell'attività di chiamata plurima da parte dei *call center*, ossia di quelle chiamate nelle quali il destinatario, dopo aver sollevato il ricevitore, non viene messo in comunicazione con alcun interlocutore (in merito v. par. 10.4): il Garante, con proprio provvedimento (6 dicembre 2011, n. 474, doc. web n. 1857326), aveva tra l'altro prescritto a due società che il contatto del destinatario di una telefonata muta non venisse richiamato per almeno trenta giorni. Il Tribunale di Roma ha confermato che il procedimento di raccolta, registrazione, consultazione, selezione, utilizzo e blocco della comunicazione che conduce alla telefonata muta è da considerarsi a tutti gli effetti un trattamento di dati personali. L'uso dei dati per una telefonata muta, inoltre, contrasta con il canone della correttezza di cui all'art. 11 del Codice, dal momento che tutto il sistema di selezione e formulazione delle chiamate passate agli operatori fa cadere il rischio e il disagio non su chi effettua la telefonata ma sui destinatari. Il giudice ha conclusivamente ritenuto che il provvedimento del Garante non fosse lesivo della possibilità di condurre campagne commerciali telefoniche, rigettando le censure di difetto di proporzionalità e ragionevolezza (sentenza 26 settembre 2013, n. 18977).

Il Tribunale di Padova ha confermato una nota con cui l'Ufficio aveva chiuso un'istruttoria preliminare, non avendo rilevato, in tema di videosorveglianza stradale, alcun profilo di violazione della disciplina posta a tutela dei dati personali. Il giudice ha ritenuto provata l'esistenza di uno specifico cartello che informava gli utenti che percorrevano il tratto di strada oggetto di controllo; a nulla è valso al ricorrente opinare che, nel senso opposto di marcia, da lui non percorso, non fosse presente alcuna segnaletica informativa. Si è infatti sottolineato che, anche in materia di tutela della riservatezza, chi agisce in giudizio non può agire a tutela della *privacy* indifferenziata degli utenti, ma solo a tutela di un proprio, specifico interesse alla protezione dei dati personali (sentenza 7 agosto 2013, n. 1330).

Il Tribunale di Roma ha invece ritenuto illecita la condotta dell'Agenzia delle dogane, la quale aveva inviato il provvedimento di trasferimento di un lavoratore, motivato sulla base di alcune indagini che la Procura della Repubblica stava svolgendo in ordine a gravi ipotesi di reato ad esso ascrivibili, non soltanto al direttore

dell'ufficio ove era impiegato, in quanto titolare del trattamento dei dati personali, ma genericamente all'ufficio, utilizzando un protocollo ordinario e non riservato e rendendo, di fatto, la nota di pubblico dominio tra i colleghi ed i superiori dell'interessato. Il giudice, discostandosi dalle valutazioni dell'Autorità (provv. 6 maggio 2010, doc. web n. 1724717), ha ritenuto che il datore di lavoro avrebbe dovuto adottare le più opportune cautele per prevenire la conoscibilità ingiustificata dei dati personali da parte di terzi, considerando infatti che, a norma dell'art. 22 del Codice, il trattamento di dati *sensibili* e *giudiziari* deve avvenire con modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato (sentenza 20 maggio 2013, n. 8437).

Il Tribunale di Torino ha confermato un provvedimento (11 ottobre 2012, n. 289, doc. web n. 2131862) con cui il Garante aveva dichiarato inammissibile un ricorso sul presupposto che il Codice non consente di chiedere la conferma di dati di cui è *sub iudice* la stessa giuridica esistenza, né di ottenere l'integrazione di informazioni o la rielaborazione delle stesse secondo modalità indicate dal ricorrente (si trattava, nel caso di specie, di una polizza assicurativa). Il giudice ha confermato che fino a quando l'esistenza del dato personale non sarà accertata con sentenza passata in giudicato, nessun diritto di accesso a tale dato potrà essere attribuito al ricorrente (ordinanza *ex* art. 702-*bis* c.p.c. del 23 aprile 2013).

È stato altresì confermato il provvedimento (17 aprile 2012, n. 149, doc. web n. 1905893) di infondatezza di un ricorso con cui un soggetto lamentava il presunto utilizzo di dati personali da parte del proprio precedente datore di lavoro, con il quale era pendente una controversia davanti all'autorità giudiziaria: il Tribunale ha ribadito, oltre alla liceità del trattamento al fine di far valere o difendere un diritto in sede giudiziaria, l'inammissibilità di richieste di tutela di dati personali meramente esplorative o congetturali (Trib. Prato, sentenza 29 marzo 2013).

In una interessante pronuncia il Tribunale di Firenze ha confermato un provvedimento inibitorio del Garante (26 ottobre 2011, n. 407, doc. web n. 1851750), reso in materia di trattamento di dati da parte di una società che si occupava di selezionare, nell'ambito di banche dati che raccolgono i dati personali di clienti di società committenti, gruppi di clienti a cui inviare *e-mail* per conto delle medesime committenti. Il Garante aveva adottato il proprio provvedimento rilevando come, non essendo stata designata la società in questione come responsabile del trattamento da parte delle committenti, essa dovesse ritenersi autonomo titolare e quindi tenuta a rendere l'informativa e ad acquisire il consenso degli interessati.

Il Tribunale ha ricordato che – per evitare che si renda necessaria una duplicazione degli obblighi informativi e di acquisizione del consenso nelle ipotesi in cui il titolare del trattamento decida di demandare a terzi la gestione dei dati – è stata prevista la possibilità di nominare per iscritto un responsabile del trattamento, la cui legittimazione al trattamento discende dall'adempimento degli obblighi di legge da parte del titolare. Il giudice ha inoltre sottolineato come costituiscano dati personali anche quelli che, pur non consentendo una identificabilità diretta, possano rendere comunque identificabile la persona a cui si riferiscono, mediante l'aggregazione dei dati relativi al sesso, alla fascia di età, alla regione e provincia di residenza e ad altre informazioni (sentenza 11 marzo 2013, n. 826).

La Corte suprema di cassazione è intervenuta in una controversia relativa alla pubblicazione, nell'ambito di un *dossier online* relativo ad alcuni soggetti, formato da una società operante nel settore delle informazioni commerciali, della notizia del fallimento di una società nella quale essi avevano ricoperto il ruolo di soci e di consiglieri di amministrazione, in epoca precedente alla dichiarazione di fallimento. Il Garante aveva accolto il ricorso degli interessati e, per l'effetto, disposto il divieto di

rendete ulteriormente disponibile l'informazione relativa alla dichiarazione di fallimento della società laddove figurasse direttamente associata agli interessati (11 febbraio 2010, doc. web n. 1705084).

In una articolata motivazione, oltre a confermare la legittimità del provvedimento opposto, il giudice della nomofilachia ha anche rammentato che la tutela dei dati personali comprende anche quelli già pubblici o pubblicati poiché colui che compie operazioni di accostamento, comparazione, esame, analisi, congiunzione, rapporto o incrocio, può ricavare ulteriori informazioni e quindi un valore informativo aggiuntivo, non estraibile dai dati isolatamente considerati, potenzialmente lesivo della dignità dell'interessato, la quale costituisce valore sommo nel nostro ordinamento. Nella gerarchia dei valori costituzionali, infatti, esso risulta preminente rispetto all'iniziativa economica privata di cui all'art. 41 della Costituzione, che infatti non può svolgersi in modo da recare danno alla dignità umana (I sez. civ., sentenza 8 agosto 2013, n. 18981).

Nel corso del 2013 è, infine, pervenuta all'Autorità una sentenza resa nel 2005 dalla Suprema Corte in tema di trattamento di dati personali nell'ambito di investigazioni difensive finalizzate a far valere un diritto in sede giurisdizionale (più esattamente, in sede di arbitrato rituale). Con provvedimento del 19 febbraio 2002 (doc. web n. 1063652) l'Autorità aveva affermato, tra l'altro, che il temporaneo differimento del diritto dell'interessato ad opporsi al trattamento ed ottenere la cancellazione dei dati è legittimo solo nel periodo in cui ciò potrebbe arrecare un effettivo pregiudizio per lo svolgimento delle investigazioni o per l'esercizio del diritto; non appena ultimate le operazioni di raccolta e trattamento e versata la relativa documentazione nel giudizio (ivi compreso quello arbitrale), non vi è più ragione di operare un ulteriore rinvio dell'esercizio dei diritti dell'interessato. Tale impostazione era stata confermata dal Tribunale di Bergamo. La Corte di cassazione, nel respingere il ricorso, ha ritenuto che tale soluzione costituisca "un ragionevole e soddisfacente punto di equilibrio tra gli interessi confliggenti, quello dell'interessato e quello degli autori e committenti della raccolta e del trattamento di tali dati" (I sez. civ. sentenza 15 luglio 2005, n. 15076).

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

Conformemente agli indirizzi giurisprudenziali e al parere espresso dall'Avvocatura generale dello Stato – che si è pronunciata in termini favorevoli alla costituzione in giudizio del Garante, ritenendo essenziale che l'Autorità possa far valere le proprie ragioni, a tutela unicamente dell'interesse pubblico, tenendo conto delle sue specifiche e caratteristiche funzioni – il Garante ha limitato la propria attiva presenza, nei giudizi che non coinvolgono direttamente pronunce dell'Autorità, 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.

18 L'attività ispettiva e le sanzioni

18.1. *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 cc.dd. provvedimenti generali.

Le ispezioni, 411 nel 2013 (cfr. sez. IV, tab. 1), sono state effettuate sulla base di programmi ispettivi semestrali secondo linee di indirizzo stabilite dal Collegio con delibere di programmazione che indicano gli ambiti del controllo e gli obiettivi numerici da conseguire. Le linee generali della programmazione dell'attività ispettiva vengono quindi rese pubbliche attraverso il sito web del Garante (cfr. *newsletter* n. 369 del 14 febbraio 2013 e n. 376 del 2 agosto 2013) e, sulla base dei criteri così fissati, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo e istruisce i conseguenti procedimenti.

Il programma relativo al primo semestre 2013 ha previsto che l'attività ispettiva fosse, tra l'altro, indirizzata nei seguenti settori:

- grandi banche dati pubbliche: per controllare i trattamenti di dati personali effettuati da enti previdenziali, mediante i propri sistemi informativi, e dall'amministrazione finanziaria, mediante il sistema informativo della fiscalità (cd. Anagrafe tributaria). Questa attività è condotta con continuità da diversi anni con lo scopo di garantire che gli accessi ai dati contenuti in queste enormi banche dati gestite da soggetti pubblici avvenga solo ed esclusivamente nel rispetto dei presupposti fissati dal legislatore e che vengano costantemente aggiornate le misure per prevenire qualunque forma di violazione della sicurezza dei dati;
- Fascicolo sanitario elettronico: (attività differita al fine di tenere presente i recenti sviluppi normativi) per rilevare l'impostazione dei trattamenti di dati personali effettuati dagli enti pubblici in relazione all'istituzione del Fse che rappresenta lo strumento di raccolta e di condivisione delle informazioni e dei documenti clinici afferenti al cittadino, generati dai vari attori del sistema sanitario;
- *telemarketing*: per accertare la liceità dei trattamenti di dati personali effettuati anche mediante sistemi automatizzati, in relazione alle attività di *marketing* telefonico realizzata mediante *call center* operanti anche all'estero. Questa attività si inserisce organicamente nel complesso di iniziative istruttorie con le quali l'Autorità si è preposta l'obiettivo di contrastare fenomeni di illecito trattamento dei dati connessi alle attività di *marketing* (che sono purtroppo ancora oggetto di frequente segnalazione);
- *mobile remote payment* (sistema che consente l'acquisto di beni digitali quali ad es., quotidiani *online*, libri elettronici, giochi, *etc.* pagando con il credito telefonico): per verificare la correttezza dei trattamenti di dati personali effettuati da tutti i soggetti coinvolti nella gestione di sistemi di *mobile payment* (in particolare, gli operatori telefonici, che mettono a disposizione il

credito disponibile sulle schede prepagate o procedono all'addebito in bolletta, nel caso degli abbonamenti; il gestore dell'infrastruttura tecnologica attraverso la quale viene fornito il servizio che consente l'acquisto; i venditori (cd. *merchant*);

- sistemi di informazione creditizia: per rilevare, attraverso ispezioni presso i principali gestori delle banche dati private in cui sono raccolte le informazioni utilizzate ai fini dell'erogazione del credito al consumo o comunque riguardanti l'affidabilità e la puntualità dei pagamenti e presso alcune società che conferiscono dati all'interno dei sistemi informativi creditizi (cc.dd. partecipanti), il rispetto e l'attualità delle misure contenute nel codice di deontologia e di buona condotta allegato al Codice, sulla base di quanto disposto con il provvedimento dell'Autorità del 16 novembre 2004.

Con riferimento, invece, al secondo semestre 2013, oltre alla prosecuzione dei controlli nei confronti degli enti previdenziali e dell'amministrazione finanziaria, l'attività ispettiva di iniziativa è stata finalizzata ad accertamenti nell'ambito di:

- *WiFi* pubblico: per esaminare le modalità e le cautele attuate dai soggetti pubblici che offrono ai cittadini l'accesso gratuito ad internet mediante connessioni *WiFi*, in particolare per quel che riguarda le misure di sicurezza implementate, la completezza delle informative sul trattamento dei dati, la rispondenza delle finalità del trattamento dei dati alla natura pubblica dell'ente che fornisce il servizio e le modalità e le garanzie con le quali gli enti pubblici hanno affidato i servizi ai soggetti privati che forniscono le infrastrutture tecnologiche;
- violazioni di sicurezza (cd. *data breach*): per constatare il rispetto, da parte dei fornitori di servizi di comunicazione elettronica, delle recenti linee guida adottate dall'Autorità in materia di *data breach* (provv. 4 aprile 2013, n. 161, doc. web n. 2388260), con particolare riferimento alla corretta gestione delle violazioni di sicurezza verificatesi e al rispetto degli obblighi di comunicazione sia nei confronti delle persone i cui dati sono stati violati, sia nei confronti del Garante che è chiamato ad effettuare una immediata valutazione sulla violazione e sulle contromisure adottate dal fornitore per attenuare le possibili conseguenze negative per gli interessati;
- attivazione di servizi non richiesti a seguito di interazione con inserzioni pubblicitarie *online* (cd. *banner*): per appurare la correttezza dei trattamenti di dati personali effettuati da società che offrono servizi a pagamento attivati a seguito dell'interazione dell'utente con collegamenti pubblicitari (*banner*) inseriti all'interno di applicazioni o pagine web. In particolare, con tale attività, tuttora in corso, si intende verificare se siano state implementate modalità di attivazione dei servizi non rispettose della volontà degli interessati con conseguente trattamento illecito dei rispettivi dati personali;
- recupero crediti: per riscontrare, alla luce dell'intensificarsi di segnalazioni concernenti le modalità operative utilizzate dagli operatori del settore, l'adeguamento da parte di questi ultimi alle prescrizioni adottate dal Garante con il provvedimento generale del 30 novembre 2005 (doc. web n. 1213644). Con questa attività, tuttora in corso, il Garante, oltre ad analizzare la liceità e la correttezza dei trattamenti effettuati, si propone di valutare l'attualità delle prescrizioni adottate nell'ottica di un loro eventuale aggiornamento.

Come specificato al successivo paragrafo 18.3, nel periodo di riferimento sono state anche effettuate in diversi settori verifiche:

- sull'adozione delle misure minime di sicurezza da parte di soggetti, pubblici e privati, che effettuano trattamenti di dati sensibili;

- concernenti l'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. Ciò, prestando anche specifica attenzione a profili sostanziali del trattamento che spiegano significativi effetti sulle persone da esso interessate.

18.2. *La collaborazione con la Guardia di finanza*

Anche nell'anno di riferimento l'Autorità si è avvalsa della preziosa collaborazione della Guardia di finanza per lo svolgimento dell'attività di controllo, in applicazione del protocollo di intesa siglato nel 2005. Al riguardo si fa rinvio a quanto nel dettaglio riferito nelle precedenti edizioni (cfr., da ultimo, Relazione 2009, p. 240 ss.), evidenziando ancora una volta la meritoria attività svolta dal Nucleo speciale *privacy*, che ha provveduto direttamente ad effettuare gli accertamenti delegati, avvalendosi anche, ove necessario, dei reparti del Corpo territorialmente competenti.

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

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

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

È proseguita l'attività di formazione del personale del Corpo al fine di approfondire la conoscenza delle disposizioni del Codice e dei provvedimenti dell'Autorità anche da parte del personale impiegato nei reparti territoriali, ordinariamente impiegato in altri servizi istituzionali.

In questo quadro, sono stati realizzati due corsi presso la Scuola di polizia tributaria, denominati "Collaborazione della Guardia di finanza con il Garante per la protezione dei dati personali", cui hanno partecipato circa quaranta tra ufficiali e ispettori.

18.3. *I principali settori oggetto di controllo*

Oltre a quanto già riportato al paragrafo 18.1, nel 2013 le ispezioni effettuate dall'Autorità hanno riguardato i titolari del trattamento che:

- hanno notificato il trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica per appurare: se il trattamento riguarda clienti o dipendenti; le modalità con le quali

gli interessati vengono informati sul trattamento e ne viene acquisito il consenso (ove necessario); nel caso in cui il trattamento sia connesso all'uso di sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro, il rispetto di quanto prescritto dal Garante nel provvedimento generale del 4 novembre 2011, n. 370 (doc. web n. 1850581) e di quanto stabilito all'art. 4 dello Statuto dei lavoratori;

- hanno notificato il trattamento di dati personali idonei a rivelare la vita sessuale o la sfera psichica degli interessati, per rilevare le modalità e le finalità del trattamento nonché le misure di sicurezza adottate;
- forniscono servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione, per verificare il rispetto di quanto stabilito dall'art 132 del Codice, con riferimento alla conservazione dei dati di traffico telefonico e telematico per finalità di prevenzione e accertamento dei reati (cd. *data retention*). In questa attività è stata posta particolare attenzione: alla verifica dei dati conservati; al rispetto dei termini tassativi di conservazione stabiliti dalla legge (il cui mancato rispetto, oltre a rendere illecito il trattamento, è sanzionato amministrativamente sia in caso di superamento del termine che di conservazione per tempi inferiori a quelli stabiliti dall'art. 132 del Codice); alla corretta attuazione delle misure e degli accorgimenti prescritti dal Garante nell'ambito del provvedimento del 17 gennaio 2008 (doc. web n. 1482111). Tra questi ricordiamo: la limitazione dell'accesso ai dati e ai locali dove gli stessi sono custoditi; il tracciamento dell'attività del personale incaricato di accedere ai dati; la conservazione separata dei dati e la loro cancellazione una volta decorso il termine di conservazione stabilito dalla legge; l'effettuazione di controlli interni sulla legittimità degli accessi ai dati da parte degli incaricati e l'adozione di sistemi di cifratura;
- raccolgono dati personali *online*, con riferimento all'iscrizione di interessati ai cc.dd. gruppi di acquisto, per accertare: la completezza delle informative rese agli interessati; la correttezza delle modalità di acquisizione del consenso; la congruenza tra le finalità indicate nell'informativa ed i trattamenti effettivamente svolti sui dati;
- sviluppano o distribuiscono applicazioni per dispositivi mobili di comunicazione (cc.dd. "*app*") per rilevare: i trattamenti di dati personali effettuati e le modalità attraverso le quali viene resa l'informativa agli interessati; la tipologia di dati raccolti al momento della registrazione dell'interessato al servizio e, successivamente, al momento dell'installazione dell'*app* sul dispositivo e durante il suo effettivo utilizzo;
- operano nel settore del *marketing*, con particolare riferimento ai trattamenti relativi alla profilazione degli interessati (cd. *market profiling*). In questo caso le verifiche hanno riguardato la tipologia dei dati raccolti, la completezza delle informative fornite agli interessati, la correttezza delle modalità utilizzate per raccogliere il consenso nonché l'effettuazione della notificazione del trattamento;
- prestano servizi di assistenza fiscale ai cittadini. Anche in questo caso le ispezioni avevano come obiettivo quello di verificare le modalità del trattamento dei dati, il rispetto degli adempimenti previsti dalla normativa e, in particolare, le misure adottate per garantire agli interessati che i dati fossero accessibili solo alle persone specificamente autorizzate e, più in generale, fossero adottate tutte le misure di sicurezza;
- operano in ambito sanitario. In questo caso si è data particolare attenzione al controllo delle modalità del trattamento con riferimento alle informative for-

nite agli interessati e alla corretta acquisizione del consenso richiesto dalla legge per il trattamento di dati idonei a rivelare lo stato di salute, nonché alla corretta gestione degli archivi (sia cartacei che informatizzati) in cui sono custoditi i dati sanitari;

- gestiscono sale giochi ove sono installati sistemi del tipo *videolottery*, con particolare riferimento alla verifica degli obblighi di informativa e consenso degli interessati i cui dati vengono raccolti dagli operatori talvolta per molteplici finalità (ad esempio fidelizzazione e *marketing*);
- forniscono servizi per il recupero di anni scolastici, con particolare riferimento al rispetto degli adempimenti connessi all'informativa che deve essere resa ai sensi dell'art. 13 del Codice all'atto della raccolta dei dati degli iscritti e alla manifestazione del consenso, quando necessario;
- gestiscono concessionarie "plurimarca" per la vendita di autoveicoli, al fine di appurare il rispetto della disciplina con particolare riferimento ai profili dell'informativa resa agli interessati nonché al consenso degli stessi, ove necessario;
- offrono servizi di intrattenimento ed effettuano trattamenti mediante sistemi di videosorveglianza, per verificare il rispetto di quanto prescritto dal Garante con il provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680).

Particolarmente rilevante per complessità e significatività di risultato è stata l'attività condotta nei confronti dei gestori delle grandi banche dati pubbliche, l'Agenzia delle entrate, con riferimento al sistema informativo della fiscalità (Anagrafe tributaria), e l'Inps.

Nel primo caso (Agenzia delle entrate) le verifiche ispettive hanno avuto ad oggetto l'acquisizione di informazioni necessarie per la definizione delle misure e degli accorgimenti che l'Autorità ha prescritto, in base all'art. 17 del Codice, a seguito della verifica preliminare richiesta dalla stessa Agenzia in relazione all'avvio dell'attività di profilazione dei contribuenti ai fini dell'accertamento sintetico del reddito delle persone fisiche di cui all'art. 38, commi 4 e 5, del d.P.R. 29 settembre 1973, n. 600, modificato dall'art. 22 del d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122 (cd. redditometro) (cfr. *supra* par. 4.7).

Con riferimento invece all'Inps, gli accertamenti hanno riguardato le modalità con le quali l'ente gestisce l'accesso da parte degli utenti esterni all'istituto (patronati, c.a.f., liberi professionisti, *etc.*) ai dati contenuti nel proprio sistema informativo, al fine di rilevare profili di criticità delle procedure, nell'ottica di incrementare le garanzie affinché i dati degli interessati siano effettivamente oggetto di trattamento solo ed esclusivamente su loro delega e per la fornitura delle prestazioni richieste. In questo caso, come per l'Anagrafe tributaria, una gestione oculata della sicurezza degli accessi, la loro tracciabilità e la rigorosa definizione dell'ambito del trattamento consentito alle migliaia di utenti abilitati costituiscono elementi essenziali per ridurre al minimo i rischi di utilizzi impropri da parte degli utenti abilitati di banche dati di particolare rilevanza e dimensioni quali sono sicuramente quelle degli enti previdenziali e dell'Anagrafe tributaria.

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

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

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

Attraverso le ispezioni l'Autorità svolge una penetrante attività istruttoria che può essere finalizzata, a seconda dei casi, 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 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).

Occorre tenere presente che, al di là della/e finalità che la sottendono, l'ispezione è pur sempre un procedimento amministrativo di controllo all'esito del quale, ove vengano accertate illiceità, l'Autorità è tenuta ad adottare i necessari provvedimenti per rendere il trattamento conforme alla legge e a contestare le sanzioni eventualmente rilevate.

Con riferimento all'anno 2013, tra i provvedimenti più rilevanti adottati dal Garante sulla base degli elementi istruttori acquisiti in sede ispettiva, si segnalano, in ordine cronologico, i provvedimenti con i quali il Garante ha:

- dichiarato illecito il trattamento dei dati personali mediante un sistema di videosorveglianza effettuato, per finalità antitaccheggio presso un esercizio commerciale, da parte di soggetti non autorizzati ad effettuare tale attività (sulla base di quanto previsto dall'art. 134, r.d. 18 giugno 1931, n. 773 Tulps), la cui osservanza costituisce presupposto di liceità del trattamento (provv. 17 gennaio 2013, n. 16, doc. web n. 2291893);
- dato specifiche prescrizioni a società esercenti l'attività di fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione, in relazione alla verifica del mancato rispetto delle misure e degli accorgimenti da adottare a garanzia degli interessati, con riferimento ai dati di traffico telefonico e telematico che tali soggetti devono conservare per finalità di accertamento e repressione dei reati (cd. *data retention*), già prescritti dall'Autorità con il provvedimento generale del 17 gennaio 2008 (doc. web n. 1482111), successivamente integrato con il provvedimento generale del 24 luglio 2008 (doc. web n. 1538237) (provv.ti 21 febbraio 2013, n. 74, doc. web n. 2338534 e 3 ottobre 2013, n. 429, doc. web n. 2740948);
- dichiarato illecito il trattamento dei dati personali effettuato da una società mediante l'utilizzo di telecamere e di un sistema di geolocalizzazione installati sui veicoli aziendali, anteriormente alla conclusione dell'accordo con le rappresentanze sindacali, con la conseguente inutilizzabilità dei dati trattati in violazione di legge ai sensi dell'art. 11, comma 2, del Codice (provv. 7 marzo 2013, n. 103, doc. web n. 2471134);
- disposto il divieto del trattamento dei dati personali acquisiti da una società mediante apparati di ripresa occultati all'interno di un rilevatore di fumo e di una lampada d'allarme nonché dichiarato illecito il trattamento dei dati personali effettuato in generale dalla stessa società a mezzo del sistema di video-

sorveglianza in quanto effettuato senza accordo con le rappresentanze sindacali, né l'autorizzazione del competente ufficio periferico del Ministero del lavoro, in violazione quindi degli artt. 114 del Codice e 4, l. n. 300/1970 (provv. 4 aprile 2013, n. 164, doc. web n. 2439178);

- dichiarato illecito il trattamento dei dati personali mediante un sistema di videosorveglianza effettuato da titolari del trattamento, pubblici e privati, in assenza dell'accordo con le rappresentanze sindacali e dell'autorizzazione del competente ufficio periferico del Ministero del lavoro, in violazione quindi degli artt. 114 del Codice e 4, l. n. 300/1970 (provv.ti 18 aprile 2013, nn. 199 e 200, doc. web nn. 2476068 e 2483269; 4 luglio 2013, n. 335, doc. web n. 2577227, n. 334, doc. web n. 2577203, n. 336, doc. web n. 2578071; 18 luglio 2013, n. 361, doc. web n. 2605290; 5 settembre 2013, n. 385, doc. web n. 2683203; 12 settembre 2013, n. 398, doc. web n. 2705679; 30 ottobre 2013, n. 483, doc. web n. 2851973 e n. 484, doc. web n. 2908871);
- disposto il divieto del trattamento dei dati personali acquisiti, per finalità di profilazione e *marketing*, in assenza del rilascio di un'idonea informativa e dell'acquisizione del necessario consenso, da parte di una società esercente l'attività di fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione (provv. 3 ottobre 2013, n. 430, doc. web n. 2745497);
- dichiarato illecito il trattamento dei dati personali effettuato da un ente pubblico per aver consentito la messa a disposizione e consultazione del fascicolo personale di una dipendente, contenente in particolare dati personali idonei a rivelare lo stato di salute dell'interessata, a soggetti non designati incaricati del trattamento, in violazione degli artt. 11, comma 1, lett. *d*), 20, commi 1 e 2, e 22, commi 3 e 5, del Codice (provv. 24 ottobre 2013, n. 469, doc. web n. 2799174);
- stabilito, nell'ambito di una verifica preliminare richiesta dall'Agenzia delle entrate, le misure e gli accorgimenti a garanzia dei diritti degli interessati sul trattamento di dati personali effettuato dall'ente richiedente ai fini dell'accertamento sintetico del reddito delle persone fisiche di cui all'art. 38, commi 4 e 5, d.P.R. 29 settembre 1973, n. 600 (cd. redditometro), modificato dall'art. 22 del d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122 (provv. 21 novembre 2013, n. 515, doc. web 2765110);
- vietato a una società il trattamento dei dati personali raccolti *online*, con finalità di intermediazione tra domanda e offerta di lavoro, in quanto risultavano effettuati in violazione di legge in assenza dell'autorizzazione prevista dal d.lgs. n. 276/2003 e sulla base di un'informativa inidonea (provv. 5 dicembre 2013, n. 547, doc. web n. 2865637);
- adottato uno schema di provvedimento recante "Provvedimento generale in materia di trattamento di dati personali nell'ambito dei servizi di *mobile remote payment*", sottoponendo a consultazione pubblica (provv. 12 dicembre 2013, n. 561, doc. web 2830145).

In molti dei provvedimenti sopra citati l'Autorità, accertata la violazione di norme del Codice per le quali la legge prevede una sanzione amministrativa, ha avviato anche un procedimento sanzionatorio. In diversi casi inoltre l'Autorità, rilevando condotte punite come reato, ha disposto anche la trasmissione degli atti alla competente Procura della Repubblica.

18.5. *L'attività sanzionatoria del Garante*

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

Nell'anno 2013, in relazione alle istruttorie effettuate, sono state inviate 71 segnalazioni di violazioni penali all'autorità giudiziaria di cui:

- ventinove per la mancata adozione delle misure minime di sicurezza;
- ventitré 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;
- tre per inosservanza di un provvedimento del Garante;
- due per falsità nelle dichiarazioni e notificazioni al Garante;
- nove in relazione ad altre violazioni penali.

Come dimostrano i dati sopra riportati (cfr. tab. 7), permangono numerose le violazioni delle misure minime di sicurezza; ciò nonostante si tratti di adempimenti di non particolare complessità, in vigore da più di dieci anni, che dovrebbero essere stati oramai "metabolizzati" sia dalle imprese che dagli enti pubblici. Deve essere nuovamente segnalata la ormai indifferibile esigenza di aggiornare il "Disciplinare tecnico in materia di misure minime di sicurezza", All. B al Codice in vigore dal 2003, le cui prescrizioni appaiono in buona parte non più adeguate allo stato dell'evoluzione tecnica, anche alla luce della ormai consistente esperienza maturata dall'Autorità in sede di controllo. Tale revisione dovrebbe essere ispirata a criteri di semplificazione, rispetto ad adempimenti di natura prettamente burocratica oggi previsti dalle disposizioni, e di maggiore effettività delle misure, prevedendo adeguati accorgimenti tecnici che intervengano in modo progressivo in funzione della quantità e della qualità dei dati, nonché della complessità della struttura tecnologica utilizzata e del numero di incaricati che vi hanno accesso.

Al di là dei risvolti sanzionatori, occorre sottolineare che la mancata osservanza delle disposizioni relative alle misure minime di sicurezza è particolarmente grave perché espone, almeno potenzialmente, i dati personali degli interessati all'accesso da parte di persone non autorizzate e a trattamenti non consentiti, intaccando il naturale affidamento degli interessati nei confronti del titolare del trattamento.

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

Come per l'anno precedente, anche nel 2013 si è avuta una notevole incidenza dell'accertamento di violazioni penali relative allo Statuto dei lavoratori connesse, nella maggior parte dei casi, all'installazione di sistemi di videosorveglianza in assenza delle garanzie previste dall'art. 4, comma 2, l. n. 300/1970. Occorre tenere presente che la disciplina prevista dallo Statuto e relativa all'utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4) e al divieto di indagini sulle opinioni ai fini dell'assunzione (art. 8), costituisce ormai parte integrante delle disposizioni del Codice (artt. 113 e 114) ed è sanzionata dall'art. 171.

L'entità delle violazioni accertate in questo settore dipende:

- dalla circostanza che pervengono all'Autorità numerose segnalazioni da parte di dipendenti o di organizzazioni sindacali;

- dalla costituzione, a partire dall'aprile del 2011 (v. p. 117 della Relazione annuale 2011) di una specifica unità organizzativa che cura anche queste istruttorie che presuppongono quasi sempre un accertamento in fatto per il quale si rende necessario lo svolgimento di ispezioni *in loco* (effettuate sia direttamente dall'Ufficio che dal Nucleo speciale *privacy* della Guardia di finanza).

18.5.2. Le sanzioni amministrative

Il dato relativo ai procedimenti sanzionatori amministrativi nell'anno 2013 (850; cfr. sez IV, tab. 6) attesta una rilevante crescita delle violazioni (+ 47% rispetto al 2012).

Per apprezzare compiutamente questo dato occorre tenere presente che all'accertamento delle violazioni amministrative previste dal Codice può procedere:

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

L'art. 13, l. n. 689/1981 prevede: "Gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro possono, per l'accertamento delle violazioni di rispettiva competenza, assumere informazioni e procedere a ispezioni di cose e di luoghi diversi dalla privata dimora, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica [...]. All'accertamento delle violazioni punite con la sanzione amministrativa del pagamento di una somma di denaro possono procedere anche gli ufficiali e gli agenti di polizia giudiziaria".

I procedimenti sanzionatori iniziano, pertanto, con la contestazione in relazione ad istruttorie effettuate direttamente dall'Autorità ma anche sulla base di accertamenti effettuati autonomamente da corpi dello Stato quali la Guardia di finanza, i Carabinieri, la Polizia di Stato che possono accertare le violazioni amministrative in materia di protezione dei dati personali in occasione di attività svolte sulla base dei propri poteri, anche di polizia giudiziaria. Questo "doppio binario" risulta complessivamente efficace, considerata l'amplissima platea di soggetti tenuti all'osservanza delle regole previste dal Codice, che renderebbe velleitario un sistema di accertamento delle violazioni accentrato solo nell'Autorità.

L'assicurazione di una uniformità di giudizio e di interpretazione è peraltro assicurata, in quanto la legge affida invece al solo Garante il compito dell'applicazione delle sanzioni in tutti i casi nei quali, a seguito dell'accertamento, il contravventore, non avvalendosi della possibilità di definire il procedimento con il pagamento entro sessanta giorni dalla notifica del doppio del minimo della sanzione, decida di proseguire il procedimento medesimo inviando scritti difensivi o chiedendo l'audizione. In tutti questi casi è infatti l'Autorità a prendere la decisione finale circa l'applicazione della sanzione adottando l'atto finale dell'ordinanza ingiunzione, quantificandone l'importo o l'archiviazione.

Le violazioni in relazione alle quali sono stati avviati procedimenti sanzionatori nel 2013 hanno riguardato (cfr. sez. IV, tab. 6):

- l'omessa o inidonea informativa – art. 161 (n. 476);
- il trattamento illecito amministrativo – art. 162, comma 2-*bis* (n. 277);
- l'omessa adozione delle misure minime di sicurezza di cui all'art. 33 del Codice – art. 162, comma 2-*bis* (n. 24);

- l'utilizzo illecito dei dati delle persone iscritte al Registro pubblico delle opposizioni per finalità di *marketing* – art. 162, comma 2-*quater* (n. 19);
- l'omessa informazione o esibizione al Garante – art. 164 (n. 18);
- l'inosservanza di un provvedimento del Garante – art. 162, comma 2-*ter* (n. 17);
- l'omessa o incompleta notificazione – art. 163 (n. 12);
- 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. 7).

Un approfondimento merita il dato relativo alle 277 violazioni di cui all'art. 162, comma 2-*bis* che si è definito "trattamento illecito amministrativo". La disposizione prevede una sanzione pecuniaria, da 10.000 a 120.000 euro in relazione alla violazione delle disposizioni di cui all'art. 167. Quest'ultima disposizione, a sua volta, richiama numerose disposizioni del Codice, estremamente eterogenee, e, in particolare, gli artt: 17 (verifica preliminare), 18, 19, 20, 21, 22, commi 8 e 11 (disposizioni concernenti il trattamento dei dati da parte di soggetti pubblici), 23, 25, 26, 27 (disposizioni concernenti il trattamento dei dati da parte dei soggetti privati), 45 (trasferimenti all'estero vietati), 123, 126, 129 e 130 (disposizioni specifiche per le comunicazioni elettroniche). Nel 2013 le violazioni concernenti il "trattamento illecito amministrativo" accertate hanno riguardato:

- in 179 casi, la violazione del consenso dell'interessato in rapporto agli artt. 23 e 130 del Codice;
- in 36 casi, violazioni commesse da enti pubblici (nella maggior parte dei casi comunicazioni o diffusioni di dati non sensibili senza i necessari presupposti di legge o regolamento);
- in 51 casi, violazioni commesse da enti pubblici con riferimento a dati sensibili;
- in 8 casi, violazioni delle misure e degli accorgimenti prescritti dal Garante nell'ambito di una verifica preliminare sulla base dell'art. 17 del Codice;
- in 3 casi, violazioni commesse da soggetti privati in relazione al trattamento di dati sensibili o giudiziari.

Analizzando i dati statistici sopra riportati si può rilevare che:

- in senso assoluto, anche per l'anno di riferimento, il maggior numero di violazioni accertate ha riguardato l'obbligo di fornire all'interessato tutte le informazioni sul trattamento dei dati, al fine di renderlo pienamente consapevole dell'effettivo utilizzo dei suoi dati personali; ciò si spiega alla luce del fatto che l'obbligo di informativa costituisce l'adempimento più generale previsto dal Codice;
- sommando le violazioni riguardanti il consenso dell'interessato (n. 179) a quelle relative all'utilizzo illecito dei dati delle persone iscritte al Registro pubblico delle opposizioni per finalità di *marketing* (n. 19), si arriva ad un totale di circa 200 violazioni commesse da soggetti privati che hanno utilizzato i dati personali dei clienti senza (o contro) la volontà degli interessati. Nella gran parte dei casi queste violazioni attengono a trattamenti effettuati da aziende per finalità di *marketing* e rientrano in quel fenomeno definito *marketing* selvaggio in relazione al quale pervengono centinaia di segnalazioni di cittadini disturbati in particolare da chiamate indesiderate sulle proprie utenze telefoniche.

Infine appare opportuno evidenziare il numero di violazioni in materia di conservazione di dati di traffico telefonico e telematico da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico per finalità di accertamento e repressione dei reati; si tratta di dati molto delicati ai quali si può accedere solo in forza di specifici decreti adottati dall'autorità giudiziaria nell'ambito delle indagini penali.

Seppure non elevato in termini assoluti (n. 7 contestazioni), il dato è rilevante se si tiene conto dell'estrema specificità di tale violazione, dell'elevata incidenza in relazione al numero di controlli effettuati (n. 12), della regolamentazione specifica e dettagliata prevista dal Codice e dai provvedimenti del Garante che evidentemente non sono stati ancora compiutamente attuati dagli operatori del settore.

I procedimenti che non si sono chiusi con il pagamento spontaneo da parte del contravventore (e sono stati quindi definiti con ordinanza dall'Autorità) sono stati 527. Di questi 420 hanno comportato l'applicazione di una sanzione (per un ammontare complessivo di somme ingiunte pari a 4.709.400 euro) e 107 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 a lei imputabile.

Tra le ordinanze più rilevanti adottate si segnalano, per rilevanza economica, quella nei confronti di una primaria società internazionale che opera nel settore della pubblicità *online* e delle ricerche web, in relazione all'omessa informativa agli interessati in conseguenza di una raccolta di dati attuata sistematicamente su tutto il territorio nazionale (ordinanza di ingiunzione del 18 dicembre 2013, n. 583, doc. web n. 2954309) e quelle nei confronti di due importanti società italiane operanti nel settore della fornitura di servizi per il *marketing*, in relazione all'utilizzo illecito di ingenti banche dati per finalità di *marketing* (ordinanza di ingiunzione del 10 gennaio 2013, n. 6, doc. web n. 2438949 e ordinanza di ingiunzione del 5 dicembre 2013, n. 549, doc. web n. 2954335). Fattore comune di queste ordinanze è stata l'applicazione della sanzione, prevista dall'art. 164-*bis*, comma 2, del Codice, a seguito dell'accertamento di plurime violazioni commesse in relazione a banche dati che possono essere qualificate "di particolare rilevanza o dimensioni", in armonia con i criteri e i principi già illustrati nella Relazione annuale 2012 (cfr. p. 265).

Per quanto invece riguarda l'interpretazione degli aspetti giuridici, si citano i seguenti casi.

- Propaganda elettorale: i trattamenti di dati personali nell'ambito di propagande elettorali, benché possano essere in senso lato assimilati alle comunicazioni commerciali tradizionali e al *marketing*, hanno una propria specificità di cui il Garante ha tenuto conto nel provvedimento generale adottato il 7 settembre 2005 (doc. web n. 1165613), attualizzato varie volte e, da ultimo, con provvedimento del 10 gennaio 2013, n. 1 (doc. web n. 2181429). L'Autorità ha definito i casi nei quali non è necessario richiedere il consenso degli elettori per l'invio del materiale di propaganda. In particolare, è stato confermato che il consenso è necessario in caso di utilizzo di particolari modalità di comunicazione elettronica come sms, mms, *e-mail* e per telefonate pre-registrate e fax, in virtù di quanto previsto dall'art. 130 del Codice. In questo ambito l'Autorità ha applicato la sanzione prevista dall'art. 162, comma 2-*bis*, del Codice, in relazione all'invio di sms di propaganda elettorale da parte di un candidato alle elezioni regionali ad una persona che aveva manifestato, in maniera espressa e specifica, la propria opposizione al trattamento. In assenza di un documentato consenso dell'interessato, il trattamento dei suoi dati personali è risultato illecito, indipendentemente dal fatto che i dati utilizzati (in questo caso il numero di cellulare) fossero stati reperiti sul web, o acquisiti nell'espletamento dell'attività istituzionale (provv. 21 febbraio 2013, n. 78, doc. web n. 2462289). Il Tribunale di Milano, pur riducendo in sede di ricorso l'ammontare della sanzione irrogata, con la sentenza del 4 dicembre 2013 ha pienamente confermato l'impostazione dell'Autorità.

- Notificazione dei trattamenti di geolocalizzazione: in ragione del fatto che la maggior parte dei sistemi *gps*, utilizzati per la geolocalizzazione, funziona mediante l'utilizzo di una scheda telefonica tramite la quale, inviando un sms, si attiva il localizzatore, indicando la posizione del mezzo sul quale è applicato, questa modalità sostanzia, così come specificato al punto 2 del parere del 23 aprile 2004 (doc. web n. 993385), il requisito della continuità di funzionamento, atteso che il sistema è in grado di fornire la posizione del mezzo (e, di regola, quantomeno indirettamente, dell'interessato) su cui è applicato il localizzatore in qualsiasi momento (cfr. provv. 18 dicembre 2013, n. 604, doc. web n. 2954181).
- I trattamenti di dati personali effettuati per mezzo di un sistema di videosorveglianza dal libero professionista persona fisica: quando il trattamento di dati personali viene effettuato, quale titolare, da una persona fisica nell'ambito della propria attività professionale non sussistono infatti le finalità esclusivamente personali che consentirebbero di escludere il trattamento dall'ambito di applicazione del Codice ai sensi dell'art. 5, comma 3, così come illustrato anche al punto 6.1 del provvedimento generale sulla videosorveglianza adottato dal Garante l'8 aprile 2010 (doc. web n. 1712680) (provv. 21 marzo 2013, n. 146, doc. web n. 2922669).
- Documentazione del consenso al trattamento dei dati personali in ambito sanitario: i trattamenti di dati personali idonei a rivelare lo stato di salute effettuati dagli esercenti le professioni sanitarie e dagli organismi sanitari pubblici rientrano tra quelli per i quali il Codice richiede il consenso informato degli interessati; in tale ambito sono previsre specifiche modalità semplificate per rendere l'informativa agli interessati medesimi ed acquisirne il consenso (art. 77). In particolare, rispetto alla regola generale che richiede la forma scritta per il rilascio del consenso al trattamento di dati sensibili (art. 23, comma 4), l'art. 81 del Codice prevede che il consenso in ambito sanitario possa essere manifestato anche oralmente ma che, in tal caso esso debba essere documentato, anziché con atto scritto dell'interessato, con annotazione scritta dell'esercente la professione sanitaria o dell'organismo sanitario pubblico. L'Autorità ha, dunque, chiarito il rapporto di genere a specie esistente tra la disposizione di cui all'art. 23, che, in quanto norma di carattere generale, individua gli elementi atti a connotare un valido consenso, e l'art. 81 che, nel caso di trattamenti in ambito sanitario, specifica le modalità con cui questo debba essere raccolto, applicando la sanzione prevista dall'art. 162, comma 2-*bis* nei confronti di un organismo sanitario che aveva omesso di documentare l'acquisizione del consenso degli interessati secondo quanto previsto dall'art. 81 del Codice (provv. 22 maggio 2013, n. 254, doc. web n. 2616474).
- Attività di *marketing* e vincolo di finalità: l'utilizzo di dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque può avvenire senza il preventivo consenso degli interessati, purché nel rispetto dei limiti e delle modalità stabilite dalla legge (art. 24, comma 1, lett. *c*), del Codice); tra questi rientra, in particolare, il cd. vincolo di finalità, in base al quale i dati possono essere raccolti e registrati per scopi determinati, espliciti e legittimi e possono essere utilizzati in altri trattamenti in termini compatibili con tali scopi, tenuto conto del dettato dell'art. 11, comma 1, lett. *b*), del Codice. Il caso riguardava una società che aveva inviato *e-mail* promozionali ritenendo erroneamente che i dati tratti da un elenco pubblico (estrapolato dal sito dell'Ordine degli avvocati) potessero essere liberamente utilizzati per finalità

di *marketing*. L'Autorità ha adottato un'ordinanza ingiunzione, ritenendo sussistente una violazione del consenso richiesto dall'art. 130, comma 2, del Codice (provv. 7 novembre 2013, n. 502, doc. web n. 2954163).

- Non applicabilità dei termini di cui alla l. n. 241/1990 ai procedimenti sanzionatori: in una ordinanza è stato ribadito che i termini indicati dalla l. n. 241/1990 non si applicano ai procedimenti sanzionatori che sono, invece, regolati dalla l. n. 689/1981. Il particolare procedimento sanzionatorio, che si conclude con l'adozione dell'ordinanza ingiunzione, prevede infatti il compimento di alcune attività necessarie, poste a garanzia degli interessati, e ne fissa le varie fasi con precise scansioni temporali, che sono incompatibili con quelle indicate nella l. n. 241/1990. Tale interpretazione è supportata dalla sentenza 27 aprile 2006, n. 9591 della Corte di cassazione civile S.U., a cui si è conformato recentemente anche il Tribunale di Milano con la sentenza 23 dicembre 2013, n. 27176/2013 (provv. 4 luglio 2013, n. 340, doc. web n. 2954141).
- Attivazione multipla di schede telefoniche: l'Autorità ha adottato numerosi provvedimenti sanzionatori in materia di attivazione multipla di schede telefoniche all'insaputa degli interessati da parte di rivenditori autorizzati (*dealer*). In particolare, poiché in numerosi casi, nell'ambito di indagini di polizia giudiziaria, era stata accertata l'assoluta inconsapevolezza dell'avvenuta attivazione in capo a coloro che ne risultavano intestatari, è stata contestata ai *dealer* che si erano resi responsabili degli illeciti la violazione dell'obbligo di informativa previsto dall'art. 161 del Codice. Nelle ordinanze adottate il Garante ha ritenuto non applicabile l'istituto del "cumulo giuridico" di cui all'art. 8 della l. n. 689/1981 – concernente il caso di chi "con un'azione od omissione viola diverse disposizioni che prevedono sanzioni amministrative o commette più violazioni della stessa disposizione" – trattandosi di azioni poste in essere dai *dealer* nei confronti di soggetti diversi e da ritenersi quindi distinte e indipendenti l'una dall'altra (provv. 18 aprile 2013, n. 204, doc. web n. 2691090).
- Inutilizzabilità dei dati tratti da liste elettorali per finalità di *marketing* in due ordinanze il Garante ha affrontato la questione della utilizzabilità, ai suddetti fini, dei dati tratti da liste elettorali acquisite prima dell'entrata in vigore del Codice (poiché con l'introduzione della nuova disciplina, vigente dal 1° gennaio 2004, l'acquisizione delle liste elettorali è consentita ai soli soggetti che utilizzino i dati per le finalità previste dall'art. 177, comma 5, fra le quali quelle connesse all'esercizio dell'elettorato attivo e passivo, al perseguimento di un interesse collettivo diffuso, alla ricerca e quelle socio-assistenziali). Nei casi portati all'attenzione dell'Autorità, due società nazionali operanti nel settore della fornitura di servizi per il *marketing*, utilizzavano dati tratti da liste elettorali, acquisite prima dell'entrata in vigore del Codice, per l'invio di comunicazioni promozionali da parte di terzi. Il Garante, nelle due ordinanze, ha confermato quanto già stabilito nel provvedimento del 10 giugno 2004 (doc. web n. 1068106), specificando che "sulla base della vigente normativa non vi è alcuna possibilità di utilizzare, per finalità di *marketing*, dati personali tratti da liste elettorali (a prescindere dall'epoca della raccolta) a meno che il titolare non dimostri di aver fornito agli interessati, in caso di acquisizione '*ante* 2004', un'idonea informativa nella quale sia reso esplicito l'utilizzo dei dati per la predetta finalità di *marketing* e di aver poi acquisito un consenso specifico per tale finalità". Il Garante ha inoltre chiarito che "le liste elettorali, sulla base della citata nor-

mativa, possono legittimamente essere acquisite solamente dai soggetti che annoverino fra le proprie finalità quelle previste dal citato art. 177, comma 5 del Codice" e non anche da imprese commerciali che si pongano quali intermediari fra i comuni che rilasciano le liste e gli enti *no-profit* che le utilizzano (provv.ti 10 gennaio 2013, n. 6, doc. web n. 2438949 e n. 549, doc. web n. 2954335).

L'ammontare dei pagamenti effettuati nell'anno 2013 da parte dei soggetti nei cui confronti sono stati avviati procedimenti sanzionatori amministrativi è risultato complessivamente pari a 4.081.760 euro di cui:

- 2.359.868 euro, pagati a titolo di definizione in via breve (entro 60 giorni dalla notifica della contestazione senza l'invio di scritti difensivi all'Autorità);
- 1.601.892 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;
- 120.000 euro, per la definizione in sede amministrativa, dei procedimenti relativi alla mancata adozione delle misure minime di sicurezza.

Gli importi relativi alle sanzioni applicate dal Garante sono versati sul bilancio dello Stato. Sulla base di quanto previsto dall'art. 166 del Codice, tali proventi, nella misura del 50% del totale annuo, sono riassegnati al fondo stanziato per le spese di funzionamento dell'Autorità previsto dall'art. 156, comma 10, del Codice e utilizzabili unicamente per l'esercizio della attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

18.6. *Le sanzioni nella proposta di regolamento europeo*

La revisione del quadro normativo comunitario in materia di protezione dei dati personali in corso a Bruxelles (e di cui si da conto nel par. 19.1) riguarderà tutta la disciplina, ivi compresi gli aspetti sanzionatori. A questo proposito, il testo dello schema di regolamento in discussione è molto più puntuale della direttiva 95/46/CE prevedendo, agli artt. 78 e 79, i criteri ai quali i legislatori degli Stati membri dovranno attenersi nella definizione del nuovo apparato sanzionatorio.

Ancorché questa parte della proposta di regolamento abbia formato oggetto di ampie discussioni nell'*iter* di approvazione sin qui percorso, si possono tuttavia trarre alcuni indici di massima che potrebbero caratterizzare il nuovo sistema sanzionatorio europeo:

- sanzioni amministrative applicate dalle autorità nazionali basate su pene pecuniarie capaci di esprimere una forte capacità dissuasiva anche per soggetti di grandi dimensioni, parametrate in percentuale al fatturato (con un limite massimo definito, nell'ultima versione, in 100.000.000 euro nel 5% del fatturato mondiale annuo);
- esimente per le violazioni non intenzionali commesse per la prima volta con invio di un ammonimento scritto;
- definizione di specifici criteri di quantificazione delle sanzioni in rapporto: alla gravità della violazione; alla natura dei dati; alla durata e all'intenzionalità o colposità della violazione; ai precedenti; alla recidività; al ravvedimento del contravventore; al nocumento causato o al fine di lucro sotteso alla violazione.

Il regolamento europeo, pur indicando ai legislatori nazionali la necessità di prevedere sanzioni amministrative efficaci, proporzionate e dissuasive, non fa nessun riferimento (come già la direttiva 95/46/CE) a possibili sanzioni di natura penale;

la loro eventuale previsione rientra nella auronomia riconosciuta a ciascuno Stato membro, che vi potrà provvedere ispirandosi a criteri di effettività, proporzionalità, capacità dissuasiva e omogeneità delle sanzioni rispetto all'apparato sanzionatorio interno e a quello degli altri Stati membri; ciò secondo un principio ormai consolidato, affermato dalla Corte di giustizia dell'Unione europea (cfr. sentenza del 21 settembre 1989, causa n. 68/88, Commissione c. Repubblica ellenica, in Racc. giur, C. giust., 1989-8, p. 2965).

In Italia, come noto, il sistema sanzionatorio in materia di protezione dei dati personali, originariamente sbilanciato a favore della sanzione penale, è stato successivamente corretto (in particolare con le modifiche intervenute con il d.l. 30 dicembre 2008, n. 207, convertito nella l. 27 febbraio 2009, n. 41) aumentando il peso delle sanzioni amministrative (ed enfatizzando così il ruolo di *enforcement* dell'Autorità chiamata ad applicarle).

Ferma restando quindi l'auronomia circa la (teorica) possibilità di sanzionare, anche penalmente, alcune (gravi) violazioni della nuova disciplina europea, appare quanto mai necessario verificare, per non eludere il primario obiettivo di armonizzazione proprio della nuova base giuridica in corso di definizione a livello comunitario, la reale necessità della conferma di tutte le (o parte delle) disposizioni che oggi prefigurano responsabilità penali conseguenti a inosservanze della disciplina, tenendo anche in considerazione gli orientamenti degli altri Paesi nella maggioranza dei quali non sono previste sanzioni penali.

Tenuto conto di queste linee generali di prospettiva e della ormai consolidata esperienza maturata sul campo dall'Autorità in questi anni, sono state definite alcune proposte di modifica all'attuale apparato sanzionatorio previsto dal Codice (e che esplicherà i propri effetti fino all'entrata in vigore del nuovo regolamento europeo che appare difficile prevedere prima di almeno tre anni) che il Garante intende proporre al legislatore e di cui si fa cenno nel prossimo paragrafo.

18.7. *Le proposte del Garante per una revisione dell'apparato sanzionatorio del Codice e l'attualizzazione delle misure minime di sicurezza contenute nell'Allegato B al Codice*

Nell'anno 2013 il Garante ha suggerito alcune modifiche (cfr. segnalazione al Parlamento del 5 luglio 2013, doc. web n. 2521783; v. *amplius* par. 2.1.1 n. 11), inizialmente inserite nel testo del disegno di legge denominato "Misure di semplificazione degli adempimenti per i cittadini e le imprese e di riordino", approvato il 21 giugno 2013 dal Consiglio dei Ministri, che si prefiggevano di apportare alcune correzioni all'attuale apparato sanzionatorio, in continuità con le tendenze generali (cui si è fatto cenno al paragrafo precedente), con l'intento tra l'altro di:

- attenuare l'impatto economico diretto e indiretto delle sanzioni mediante accesso a formule di estinzione particolarmente favorevoli (pagando direttamente il minimo della sanzione) quando la violazione è commessa per la prima volta da soggetti che rientrano nella definizione di piccola e media impresa o da enti pubblici di piccole dimensioni (es. piccoli comuni);
- eliminare l'attuale duplicazione di sanzione (amministrativa e penale) in caso di violazione colposa delle misure minime di sicurezza, limitando la violazione penale solo al caso in cui, a causa dell'inadeguatezza delle misure di sicurezza adottate, si verifichi "la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati", abrogando contestualmente la procedura del cd. ravvedimento operoso attualmente prevista dall'art. 169, comma 2, del Codice.

Queste modifiche appaiono ancora oggi necessarie e utili nell'ottica di bilanciare ulteriormente un assetto che, nell'esperienza quotidiana dell'Autorità, appare talvolta eccessivamente pesante nei confronti di violazioni minori, con una ricaduta ridotta in termine di lesione effettiva dei diritti.

Per altro verso, invece, l'esperienza applicativa dell'Autorità dimostra che, in ambiti nei quali gli interessi economici e la competizione sul mercato tra soggetti diversi sono molto forti, l'attuale sistema sanzionatorio risulta scarsamente dissuasivo (il caso tipico è quello del fenomeno del cd. *marketing* selvaggio).

In questi casi si rende necessario semmai introdurre forme di progressivo automatico aggravamento delle sanzioni in caso di ripetute violazioni delle medesime disposizioni da parte dello stesso soggetto in un arco di tempo definito, al fine di disincentivare le pratiche scorrette.

Come già evidenziato al precedente paragrafo 18.5.1, ormai indifferibile appare la revisione delle misure minime di sicurezza contenute nel disciplinare tecnico allegato B al Codice, in ragione dell'obsolescenza di molte disposizioni (pensate ormai più di dieci anni fa) e del mutato contesto tecnologico di riferimento, con l'esigenza crescente di proteggere il dato non solo staticamente, allorché è memorizzato all'interno di una banca dati, ma, ancor di più, in tutte le occasioni (sempre più frequenti) in cui lo stesso è oggetto di trasferimenti per mezzo delle reti di comunicazione o di accesso da parte di postazioni remote.

Il processo di revisione di queste regole è affidato dalla legge (art. 36 del Codice) ad un decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie e il Ministro per la semplificazione normativa.

Nel disegno di legge "Misure di semplificazione degli adempimenti per i cittadini e le imprese e di riordino normativo", attualmente all'esame del Senato, è già prevista una modifica di questa norma, ma non nel senso auspicato dall'Autorità.

Considerata la particolare sensibilità e l'esperienza maturata sul campo nelle centinaia di ispezioni effettuate nei più diversi contesti tecnologici, apparirebbe più opportuno infatti affidare al Garante non solo un ruolo consultivo ma di iniziativa dell'*iter* di rinnovamento di quelle misure di minime di sicurezza la cui corretta implementazione, da parte di enti pubblici e soggetti privati, costituisce ormai una condizione necessaria ed essenziale di garanzia per i cittadini nella società dell'informazione, restituendogli anche il potere di semplificare tali misure in tutti quei contesti in cui la loro implementazione risulterebbe sproporzionata in relazione alla tutela degli interessi protetti.

19 Le relazioni comunitarie e internazionali

Il 2013 è stato un anno cruciale per la protezione dei dati a livello europeo e internazionale.

Sono infatti proseguite le intense attività di revisione degli strumenti normativi più importanti in materia, nell'ambito dell'Unione europea, del Consiglio d'Europa e dell'OCSE, dettate dalla necessità di rispondere alle numerose sfide poste dall'incessante sviluppo tecnologico e dalla globalizzazione, nonché dall'esigenza di pervenire a *standard* uniformi nei diversi stati.

L'Autorità ha contribuito attivamente a tali processi di riforma partecipando ai numerosi gruppi di lavoro istituiti in ambito UE ed internazionale (cfr. tabelle 1 e 21).

In particolare, a livello comunitario è proseguito il negoziato riguardo ad un nuovo quadro giuridico europeo sulla protezione dei dati, composto dalla proposta di regolamento generale (doc. web n. 2110215), volto a sostituire la direttiva 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali), e dalla proposta di direttiva sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzioni di sanzioni penali (settori attualmente esclusi dall'ambito di applicazione della direttiva 95/46/CE) (doc. web n. 2110225).

L'attività legata al regolamento (v. par. 19.1) è proseguita in maniera assai intensa anche in vista dell'imminente fine della legislatura del Parlamento europeo e della scadenza del mandato della Commissione, previste entrambe per il 2014. L'auspicio è di pervenire, prima della fine della legislatura, ad un testo condiviso eventualmente da perfezionare durante il semestre di Presidenza italiana (luglio-dicembre 2014).

In linea generale, il dibattito sulla proposta di direttiva è andato più a rilento rispetto a quello che ha interessato la proposta di regolamento, anche in ragione del fatto che si è ritenuto opportuno risolvere preliminarmente le questioni problematiche in sede di regolamento generale, per poi esaminare l'eventualità di riproporre, laddove opportuno, le soluzioni raggiunte nella direttiva (v. par. 19.1).

Parallelamente al pacchetto di riforma UE, nell'ambito del Consiglio d'Europa è proseguito il processo di modernizzazione della Convenzione 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale. Con l'approvazione del documento finale contenente le proposte di revisione della Convenzione 108 da parte del Comitato consultivo T-PD, avvenuta alla fine del 2012, si è conclusa la fase tecnica del lavoro di modernizzazione della 108 e si è aperta una fase "politica", con l'istituzione di un comitato intergovernativo (CAHDATA) incaricato dal Comitato dei Ministri del Consiglio d'Europa di portare a termine la stesura di un protocollo emendativo alla Convenzione (v. par. 19.5).

In sede OCSE, si è invece concluso il processo di modernizzazione degli strumenti *privacy* avviato nel 2010, con l'adozione, avvenuta l'11 luglio 2013, delle nuove linee guida *privacy* OCSE che sostituiscono quelle del 1980 (v. par. 19.5).

Sia a livello europeo che internazionale, il 2013 si è anche caratterizzato per l'importante lavoro svolto dalle Autorità di protezione dei dati finalizzato ad una più stretta ed efficace cooperazione, specie in materia di *enforcement* (v. *infra*). L'accentuarsi della natura transfrontaliera delle problematiche legate all'attuazione dei principi di protezione dei dati nel mondo digitale rende infatti necessaria la predisposizione di strategie comuni sulla base di principi condivisi.

19.1. *La riforma del quadro giuridico europeo in materia di protezione dei dati*

La riforma del quadro giuridico in materia di protezione dati nell'UE proposta dalla Commissione europea il 25 gennaio 2012 comprende un regolamento generale sulla protezione dei dati ed una direttiva che disciplinerà i trattamenti di dati personali svolti per finalità di contrasto dei reati. L'adozione dei testi definitivi avverrà dopo l'approvazione da parte dei due co-legislatori (Parlamento europeo e Consiglio dell'UE), secondo la procedura introdotta dal Trattato di Lisbona.

Nel corso del 2013, l'Autorità ha continuato a partecipare attivamente al negoziato in corso al Consiglio UE, assicurando un costante flusso di contributi scritti sull'articolato del testo e contribuendo alla definizione della posizione italiana nel negoziato. I lavori del gruppo del Consiglio che esamina il pacchetto si sono concentrati principalmente sulla proposta di regolamento, giunta alla terza/quarta lettura, anche se nulla sarà definito finché non si sarà trovato l'accordo su tutto l'articolato. Pertanto alcune parti sono state analizzate più dettagliatamente per scelta delle presidenze che si sono succedute nel corso dell'anno, nel tentativo di giungere ad un comune sentire rispetto ad aspetti fondamentali e nuovi della proposta come il principio del cd. *one stop shop* (sportello unico) ed i meccanismi di mutuo riconoscimento.

La proposta di direttiva, per la quale si è arrivati alla seconda lettura di parte del testo, essendo in parte legata alla soluzione di temi generali (definizioni, principi fondamentali, obblighi dei titolari, trasferimento dei dati, supervisione e controllo) ed in parte legata ad istanze legate al mantenimento della sovranità degli Stati in ambiti quali la prevenzione, contrasto e repressione di crimini, ha avuto finora un percorso più lento.

L'intento perseguito dal Garante nella partecipazione ai lavori sul pacchetto di riforma UE è, in primo luogo, quello di assicurare che i nuovi strumenti in discussione non contengano previsioni peggiorative rispetto a quelle contenute nella direttiva 95/46/CE, recepite nella legislazione italiana, prima con la l. n. 675/1996 e, poi, con il Codice. Uno dei principali propositi della riforma UE è infatti quello di mantenere alto il livello di tutela dei diritti delle persone, pur nella semplificazione degli oneri per imprese e altri soggetti titolari del trattamento. In quest'ottica, appare ad esempio auspicabile che il perseguimento del cd. sportello unico – che individua un'unica autorità di controllo competente a controllare le attività del titolare del trattamento in tutta l'Unione, in modo da garantire la certezza giuridica e ridurre gli oneri amministrativi per i titolari del trattamento – sia accompagnato da meccanismi che rendano altrettanto agevole l'esercizio dei diritti da parte degli interessati (cd. *proximity*). Appare inoltre auspicabile che con il nuovo pacchetto di riforma si arrivi ad un quadro di sanzioni, in caso di mancato rispetto dei principi di protezione dei dati, il più possibile uniforme tra i vari Stati.

Quanto ai tempi della riforma, contrariamente a quanto auspicato anche dal Gruppo Art. 29 nella lettera alla Presidenza greca dell'11 dicembre 2013 (doc. web n. 2980372) ovverosia, l'adozione del pacchetto di riforma entro la fine della legislatura UE, il documento finale del Consiglio UE del 25 ottobre 2013 ha genericamente fatto riferimento ad una "tempestiva adozione" del pacchetto di protezione dati per consentire il pieno funzionamento del mercato unico digitale "entro il 2015". Il Garante ha a tal proposito manifestato la propria delusione auspicando invece una risposta all'altezza delle aspettative.

Va ricordato, peraltro, il voto del 21 ottobre con cui la Commissione competente del Parlamento europeo (LIBE - Libertà civili, giustizia e affari interni) ha approvato gli emendamenti ai testi delle due proposte (regolamento e direttiva).

A questo voto, giunto dopo oltre 20 mesi di intenso dibattito durante i quali sono stati presentati più di 3.000 emendamenti, ha fatto seguito la votazione finale della Plenaria avvenuta il 12 marzo 2014. Se anche l'altro co-legislatore europeo (il Consiglio UE) arriverà ad un accordo politico sul testo dei due strumenti, potranno avere inizio i negoziati attraverso il cosiddetto "trilogo" fra Parlamento, Consiglio e Commissione, auspicabilmente, sotto presidenza italiana, nel secondo semestre del 2014.

Il Parlamento ha mantenuto chiara l'impostazione iniziale ovvero che le due proposte fanno parte di un "pacchetto" di norme da gestire in modo unitario; per tale ragione molti emendamenti alla proposta di direttiva sui trattamenti di dati personali nelle attività giudiziarie e di polizia tendono a garantire uniformità con le disposizioni introdotte nel regolamento che fissa un quadro "generale" di norme in materia di protezione dati nell'UE: ciò vale, ad esempio, rispetto alle definizioni contenute nei due strumenti, ai poteri delle autorità di controllo, alla loro previa consultazione o ad alcuni strumenti (quali la valutazione di impatto-*privacy*).

Per quanto riguarda gli emendamenti approvati relativi alla proposta di regolamento, il testo mantiene in larga parte l'impostazione dell'originaria proposta della Commissione: ad esempio, in materia di consenso della persona interessata (che deve essere "esplicito" anziché solo "inequivocabile" come nell'attuale direttiva 95/46/CE) o in tema di diritto alla portabilità dei dati. Sono state inoltre mantenute, sia nel testo del regolamento che in quello della direttiva, alcune proposte innovative, quali la nomina (obbligatoria) di un "*data protection officer*" da parte di alcune categorie di titolari di trattamento (secondo criteri però diversi rispetto a quelli indicati dalla Commissione), l'introduzione di un obbligo generale per tutti i titolari di notificare eventuali violazioni di dati personali (anche agli interessati, in determinati casi), e, per altro verso, l'eliminazione dell'obbligo, oggi vigente, di notificare i trattamenti all'autorità di controllo. Gli emendamenti introducono anche versioni "semplificate" di alcune disposizioni del futuro regolamento: ad esempio, il diritto all'oblio è stato trasformato in un diritto alla rettifica o al "congelamento" dei dati.

La posizione della LIBE è stata influenzata anche dalla necessità di fornire risposte "forti" alle attività di sorveglianza di massa legate al cd. *Datagate* trapelate sugli organi di stampa a partire dal giugno 2013. Così si spiega, ad esempio, la scelta di vincolare all'autorizzazione dell'autorità di protezione dei dari competente nonché alla preventiva informativa all'interessato, l'invio di dati su richiesta di autorità giudiziarie o amministrative di Paesi terzi.

Il voto LIBE ha fornito una spinta al rafforzamento dei diritti degli interessati, nonché alla previsione di forti sanzioni per le imprese che violino i principi di protezione dei dati personali. Nel testo approvato è stato infatti modificato il sistema delle sanzioni amministrative, che tutte le autorità nazionali di controllo devono poter comminare, ma che sono libere di definire entro una soglia pecuniaria massima e nel rispetto di una griglia di criteri fissati nel resto, cui si aggiunge l'intervento chiarificatore e di indirizzo del Comitato europeo della protezione dati (il *board* europeo della protezione dati, "erede" dell'attuale Gruppo Art. 29). Ulteriori modifiche significative riguardano il cd. sportello unico e la collaborazione fra autorità di controllo attraverso il cd. meccanismo di coerenza: secondo il Parlamento, lo sportello unico deve permettere alle imprese multinazionali di dialogare con un unico interlocutore nell'UE (l'autorità di controllo del Paese dove hanno lo "stabilimento principale"), ma il ruolo di questa autorità capofila (cd. *lead authority*) deve consistere nel coordinamento di un processo di co-decisione cui tutte le autorità degli Stati membri interessati da un trattamento devono partecipare.

Gli aspetti che hanno suscitato perplessità in entrambi gli strumenti così come emendati nelle proposte della LIBE riguardano invece l'introduzione della definizione di "dato pseudonimo", locuzione suscettibile di generare incertezze interpretative; le norme sulla profilazione e la definizione stessa di profilazione; l'introduzione, chiesta dal Parlamento (ma solo nel regolamento), di un "certificato europeo" della protezione dati, che costituisce una sorta di "bollino-qualità" in grado di consentire ai titolari di trattamenti di beneficiare di varie deroghe ed esenzioni, e la cui vigilanza sarebbe affidata a soggetti terzi, diversi dalle autorità di controllo. Tali aspetti appaiono peraltro tra i punti (critici) evidenziati anche dal Gruppo Art. 29 che, nell'allegato alla citata lettera alla presidenza greca dell'11 dicembre 2013, ha sottolineato gli aspetti ancora migliorabili della riforma.

In tale sede il Gruppo ha comunque manifestato il proprio plauso al lavoro svolto dalla LIBE, che ha tenuto conto di molte delle raccomandazioni fornite dallo stesso WP29, ha perseguito l'idea del "pacchetto di riforma" votando su entrambe le proposte della Commissione (regolamento e direttiva) e non ha lasciato dubbi sul fatto che il regolamento si applichi tanto al settore privato quanto a quello pubblico.

Più in generale, il Gruppo Art. 29 ha seguito con attenzione il processo di riforma in atto, fornendo diversi contributi nel corso dell'anno. In particolare, nel parere n. 1/2013 adottato il 26 febbraio 2013 (doc. web n. 2980389), completando il lavoro fatto nel 2012 con i pareri nn. 1/2012 e 8/2012 (doc. web nn. 2572831 e 2133818; cfr. Relazione 2012, p. 273), si è soffermato sulla proposta di direttiva della Commissione, ed in particolare sulla necessità di: rafforzare la tutela dei dati relativi a persone non sospette, vittime di reati e terze parti; ampliare l'esercizio dei diritti dell'interessato che non deve essere oggetto di deroghe ingiustificate; applicare il principio della verifica dell'impatto *privacy* anche nell'ambito della direttiva; rafforzare e specificare i poteri delle autorità di protezione dati in questo particolare ambito.

Con il documento del 27 febbraio 2013 (doc. web n. 2980331) il Gruppo ha preso posizione su sei specifici settori del pacchetto di riforma, ed in particolare sulla necessità di: mantenere un approccio omogeneo sul trattamento di dati effettuati in ambito privato e pubblico; considerare i "dati pseudonimi" come dati personali (applicando quindi anche ad essi i principi di protezione dati); specificare che il consenso dell'interessato deve essere "esplicito"; irrobustire il ruolo delle autorità nazionali di protezione dei dati – rispetto alle quali l'imprescindibile requisito dell'indipendenza è stato ribadito dalla Corte di giustizia nella sentenza dell'8 aprile 2014 (Commissione europea c. Ungheria) (Causa C-288/12) – e del Comitato europeo della protezione dati; rafforzare la tutela dei dati che siano oggetto di trasferimento verso Paesi terzi; mantenere l'approccio fondato sulla valutazione del rischio da parte dei titolari del trattamento. Nei due allegati a tale documento il Gruppo ha altresì dedicato una particolare attenzione al tema della cd. *household exemption* ovvero la deroga ai principi di protezione dei dati ove il trattamento sia limitato a finalità esclusivamente personali (doc. web n. 2980411) e della cd. *lead authority* e delle sue competenze (doc. web n. 2980401).

Il Gruppo ha anche preso posizione sulla disciplina in materia di profilazione contenuta nella proposta di regolamento. Con l'*advice paper* del 13 maggio 2013 (doc. web n. 2980350) ha fornito indicazioni affinché nella proposta di regolamento sia garantita una maggiore trasparenza e un più efficace controllo sui propri dati da parte dell'interessato, una più ampia responsabilità dei titolari che intendano avvalersi di tecniche di profilazione, ed un approccio flessibile del testo normativo capace di fornire una tutela appropriata distinguendo le ipotesi di profilazione che abbiano ripercussioni sui diritti delle persone e quelle invece caratterizzate da un livello di intrusione meno significativo.

19.2. *Le conferenze delle Autorità su scala internazionale*

La Conferenza internazionale delle autorità di protezione dati si è tenuta a Varsavia dal 23 al 26 settembre 2013.

La Conferenza internazionale delle autorità di protezione dati

La Conferenza di quest'anno, alla quale hanno partecipato il Presidente e il Segretario generale dell'Autorità, si è articolata su tre macro-aree tematiche: i processi di revisione degli strumenti di protezione dei dati attualmente in corso a livello europeo e internazionale (UE, Consiglio d'Europa, e OCSE); le sfide per la *privacy* sollevate dalle nuove tecnologie; le prospettive, il ruolo e gli interessi dei diversi attori in gioco.

Nel corso della Conferenza sono state adottate otto risoluzioni. Particolare interesse riveste la risoluzione, sostenuta anche dal Garante, con la quale la Conferenza ha adottato un programma comune che impegna i governi a promuovere l'educazione digitale di tutti i cittadini, senza distinzione di età, esperienza o ruolo rivestito (doc. web n. 2681083). Il programma fissa cinque principi: assicurare una protezione particolare ai minori; garantire una formazione permanente sulla tecnologia digitale; raggiungere un giusto equilibrio tra opportunità e rischi presenti in tale ambito; promuovere il rispetto degli utenti; diffondere un pensiero critico sull'uso delle nuove tecnologie. Le altre Risoluzioni hanno invece riguardato: la necessità che imprese e governi assicurino la massima trasparenza nel trattamento dei dati dei cittadini (doc. web n. 2674966); l'esigenza che l'attività di profilazione si basi su una preliminare valutazione di impatto-*privacy*, garantisca trasparenza agli interessati e ponga particolare attenzione alla tutela dei minori (doc. web n. 2674994); l'attenzione da porre ai rischi legati al crescente ricorso al tracciamento della navigazione sul web (cd. *web tracking*), che deve essere reso più trasparente ed ispirarsi ai principi detti di *privacy by design* (doc. web n. 2675046); l'obiettivo di pervenire ad un maggiore coordinamento tre le autorità per aumentare l'efficacia delle attività di *enforcement* (doc. web n. 2681271); l'esigenza di adottare un piano strategico di azione per il biennio 2014-2015 finalizzato alla creazione di una rete globale di regolatori (doc. web n. 2674167); la necessità di un accordo internazionale vincolante che salvaguardi i diritti umani attraverso un corretto equilibrio tra sicurezza, interessi economici e libertà di espressione (doc. web n. 2674346). La Conferenza ha anche adottato una dichiarazione sui rischi e le sfide posti dal crescente uso delle *app*, che ha assunto dimensioni tali da poter parlare di una vera e propria "appificazione" della società (doc. web n. 2659319).

A margine della Conferenza internazionale si è tenuto il primo *workshop* del progetto europeo PHAEDRA (*Improving Practical and Helpful cooperAtion bEtween Data PRotection Authorities*) volto a migliorare la cooperazione tra le autorità di protezione dei dati. Per il secondo anno di attività, lo stesso si soffermerà su due aspetti problematici: la creazione di un quadro (vincolante o meno) per lo scambio di informazioni nonché per le ispezioni congiunte e l'individuazione degli ostacoli alla cooperazione e di possibili soluzioni (v. anche par. 19.5).

La Conferenza delle autorità europee (*Spring Conference*)

L'annuale Conferenza di primavera (*Spring Conference*) che riunisce le autorità di protezione dei dati europee, svoltasi a Lisbona dal 16 al 17 maggio, ha approvato tre importanti risoluzioni con le quali vengono fissate precise condizioni necessarie a tutelare i cittadini europei in particolare rispetto agli scenari futuri della *privacy*, al negoziato per la creazione di un'area di libero scambio USA-UE e ai trattamenti di dati effettuati da Europol.

La prima Risoluzione (doc. web n. 2980494), che concerne il futuro della protezione dei dati personali in Europa, sottolinea l'urgenza che il nuovo Regolamento generale sulla protezione dei dati e la proposta di direttiva siano adottati contestual-

mente per evitare pericolose lacune nella tutela dei cittadini europei, in particolare in un momento di crescente accesso ed uso da parte di autorità giudiziarie e forze di polizia di dati personali raccolti ed in possesso di soggetti privati. La Risoluzione incoraggia inoltre sia le imprese, sia le istituzioni pubbliche ad investire nella sicurezza dei dati e le autorità di protezione dati a cooperare tra loro.

La seconda Risoluzione (doc. web n. 2980484), promossa dall'autorità tedesca ed appoggiata tra gli altri dal Garante, tocca il delicato tema della creazione di uno spazio transatlantico di libero scambio ed auspica che nelle prossime negoziazioni tra UE ed USA il diritto fondamentale alla protezione dei dati venga promosso attraverso regole, sia sostanziali sia procedurali, volte a disciplinare lo scambio di dati e consentire controlli efficaci da parte di autorità indipendenti, anche per quanto riguarda l'accesso da parte delle autorità giudiziarie e di polizia alle banche dati delle imprese.

La terza Risoluzione (doc. web n. 2980604), che ha avuto anch'essa tra i proponenti il Garante, è dedicata al nuovo quadro legale presentato dalla Commissione europea che ridisciplina funzionamento e competenze dell'Europol, introducendo novità di grande rilievo ed impatto (ampliamento dei reati per i quali l'organizzazione è competente a raccogliere ed analizzare dati; crescita delle possibilità di comunicazione ed accesso ai dati all'interno ed all'esterno dell'organizzazione). La Risoluzione mira a scongiurare il rischio che le proposte della Commissione abbassino il livello di tutela rispetto a quello oggi vigente, impedendo il rispetto di principi essenziali (in particolare quello di finalità) che oggi limitano il riutilizzo e l'accesso ai *file* e alle informazioni talora sensibili detenute da Europol.

19.3. *La cooperazione tra Autorità garanti nell'UE: il Gruppo Art. 29*

La cooperazione tra le Autorità garanti nell'UE riunite nel Gruppo Art. 29 è proseguita nel 2013 coerentemente al programma di lavoro adottato il 1° febbraio 2012 (doc. web n. 2375271).

L'obiettivo principale del Gruppo non è stato solo quello di assicurare una corretta e coerente applicazione del sistema di protezione dei dati in vigore, ma anche di proseguire il lavoro di preparazione rispetto al futuro quadro normativo sulla base delle proposte della Commissione europea del 25 gennaio 2012 (cfr. *supra* par. 19.1).

Punto chiave del lavoro dei Garanti è stata anche la riflessione su strategie comuni di *enforcement* volte a rendere più efficace l'applicazione dei principi di protezione dei dati su scala internazionale.

Inoltre il lavoro del Gruppo si è concentrato sulle numerose sfide che derivano dall'incessante sviluppo delle nuove tecnologie, sulla necessità che anche nell'ambito della libertà, sicurezza e giustizia sia assicurato un efficace sistema di tutela dei diritti degli individui, sulle sfide della globalizzazione e sul tema dei trasferimenti internazionali di dati.

Il Gruppo si è riunito in sessione plenaria cinque volte. Il lavoro preparatorio è stato svolto, come di consueto, nei sottogruppi tematici a cui l'Autorità ha attivamente partecipato.

Applicazione uniforme delle norme-chiave della direttiva 95/46/CE

Il Gruppo ha proseguito il suo lavoro sulla corretta interpretazione ed applicazione delle nozioni fondamentali della direttiva 95/46/CE con il sottogruppo denominato "*Key Provisions*". In particolare, l'attività si è concentrata sull'approfondimento del concetto di finalità del trattamento e di trattamento compatibile con l'adozione del Parere n. 3/2013 (doc. web n. 2572901).

In tale parere il Gruppo da una parte ha svolto un'analisi dettagliata del principio di finalità previsto dall'art. 6, comma 1, lett. *b*), direttiva 95/46/CE (offrendo indicazioni specifiche sulla sua applicazione alla luce del quadro normativo vigente), dall'altra ha rivolto raccomandazioni al legislatore europeo affinché il nuovo regolamento mantenga le necessarie garanzie a presidio dei diritti delle persone.

Parere sul principio di finalità

Il principio di finalità è in effetti un elemento cruciale della tutela dei dati. Tale principio, che determina i limiti dell'uso dei dati da parte dei titolari del trattamento (consentendo comunque un certo grado di flessibilità), è caratterizzato da due componenti principali: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime ed essere successivamente trattati in modo non incompatibile con tali finalità (cd. uso compatibile). La valutazione della compatibilità, da effettuarsi caso per caso, deve tenere conto delle circostanze pertinenti ed in particolare: del rapporto tra gli scopi per i quali i dati sono stati raccolti e le finalità di trattamento successivo; del contesto in cui i dati personali sono stati raccolti e delle ragionevoli aspettative degli interessati riguardo al loro ulteriore utilizzo; della natura dei dati personali e dell'impatto del trattamento ulteriore sugli interessati; delle misure di salvaguardia adottate dal titolare per garantire un trattamento equo ed evitare eccessive ripercussioni sugli interessati.

Nel parere il Gruppo ha preso posizione su un aspetto importante del principio di finalità del trattamento, chiarendo che il trattamento di dati incompatibile con le finalità della raccolta è illecito. Il titolare non può dunque legittimare tale trattamento semplicemente avvalendosi di una nuova base giuridica prevista dall'art. 7 della direttiva. Il principio di finalità può infatti essere limitato solamente alle strette condizioni previste dall'art. 13 della direttiva, quando cioè tale restrizione, prevista per legge, costituisce una misura necessaria a salvaguardare gli specifici interessi previsti dallo stesso art. 13. Una simile posizione è parsa necessaria a fronte della proposta di Regolamento della Commissione che all'art. 6, comma 4 prevede un'ampia eccezione al principio di compatibilità stabilendo che se lo scopo dell'ulteriore trattamento non è compatibile con quello per il quale i dati personali sono stati raccolti, il trattamento deve avere come base giuridica almeno uno dei requisiti di legittimità del trattamento (previsti attualmente dall'art. 7 della direttiva) fatta eccezione per il "legittimo interesse" del titolare.

Proprio la sussistenza di un "legittimo interesse" in capo al titolare del trattamento, una delle possibili basi giuridiche su cui fondare il trattamento dei dati (in alternativa, ad esempio, al consenso dell'interessato), è stato un altro tema chiave della direttiva 95/46/CE affrontato nel corso dell'anno dal sottogruppo *Key Provisions*. In base all'art. 7, lett. *f*), della direttiva il trattamento di dati personali può essere effettuato ove sia necessario per il perseguimento dell'interesse legittimo del titolare del trattamento oppure dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata.

Parere sul "legittimo interesse"

Il tema è parso di particolare rilevanza anche alla luce del fatto che la proposta di Regolamento, introducendo l'obbligo di cd. *accountability*, tende a rafforzarne l'uso lasciando allo stesso titolare la valutazione sulla prevalenza del legittimo interesse sui diritti dell'interessato (il Codice prevede invece che il "bilanciamento" sia operato dal Garante (cfr. art. 24, comma 1, lett. *g*).

Secondo il Gruppo, il legittimo interesse costituisce un criterio di legittimità che non necessariamente deve applicarsi in via residuale, quando cioè non sia possibile avvalersi degli altri requisiti di legittimità del trattamento previsti dall'art. 7. Al contrario, può risultare il criterio più congruo – purché siano rispettati i diritti fondamentali dell'interessato – per evitare di fondare il trattamento su requisiti che non forniscano sufficienti garanzie per l'interessato (si pensi ad esempio all'ambito lavorativo, ove il

consenso del dipendente, a fronte del rapporto di per sé squilibrato tra datore di lavoro e lavoratore, difficilmente può dirsi "libero" come invece richiesto dalla direttiva).

Occorre tuttavia evitare accuratamente che il legittimo interesse possa rappresentare la facile via d'uscita per il titolare che non abbia altra base su cui fondare il trattamento.

Per tale ragione il parere in corso di elaborazione dovrà essere sufficientemente "prescrittivo" nell'individuazione dei criteri su cui basare il bilanciamento di interessi in gioco.

Anche in questo caso, l'impostazione finora data dal sottogruppo al parere si struttura su un'accurata analisi del testo dell'art. 7, lett. *f*), della direttiva e su una parte conclusiva contenente possibili raccomandazioni riguardo alla normativa in materia, con particolare riferimento al pacchetto di riforma attualmente in discussione.

Aeromobili a pilotaggio remoto (cd. droni)

Molto intensa è stata l'attività del Gruppo Art. 29 con riferimento alle sfide per la protezione dei dati sollevate dalle nuove tecnologie. In questa cornice, è stata predisposta ed inviata alla Commissione europea una risposta ad un questionario sugli aspetti di riservatezza e protezione dei dati correlati all'utilizzo di aeromobili a pilotaggio remoto (APR, cd. droni) in ambito pubblico, commerciale e privato (doc. web n. 2982766).

Il questionario era stato inoltrato al Gruppo Art. 29 dalla Commissione (DG imprese e industrie) nell'ambito di un progetto volto a integrare tali mezzi nel piano di gestione del traffico aereo europeo (ATM-*Air Traffic Management*) al fine di aprire un confronto con le autorità di protezione dei dati europee sul tema. Il Garante, in qualità di *rapporteur*, ha raccolto le risposte fatte pervenire dalle diverse autorità e ha predisposto la lettera volta a sintetizzarne il contenuto e a richiamare l'attenzione su alcuni aspetti problematici del trattamento dei dati personali (base giuridica, informativa, titolarità del trattamento, *etc.*) effettuato attraverso i sempre più avanzati sistemi di rilevazione con cui tali mezzi possono essere equipaggiati (microfoni e telecamere ad alta risoluzione e/o per la visione termica notturna, strumenti per intercettare le comunicazioni *wireless*, *etc.*). Il tema dovrebbe essere comunque oggetto di ulteriore approfondimento per la predisposizione di uno specifico parere, considerato che la Commissione europea intende adottare una comunicazione contenente proposte tese ad incentivare l'uso di tali apparecchi a fini commerciali.

Parere sulle *mobile apps*

Sempre in tema di nuove tecnologie, con l'adozione del Parere n. 2/2013 (doc. web n. 2572891), predisposto dal sottogruppo *Technology*, si è concluso il lavoro iniziato nel 2012 sui profili di protezione dei dati nell'ambito delle applicazioni per telefonia mobile (cd. *mobile apps*). Il parere, di cui il Garante è stato correlatore con specifico riferimento al profilo della sicurezza, evidenzia le problematiche emerse in seguito all'esponenziale diffusione delle applicazioni su dispositivi mobili degli ultimi anni.

Attraverso le *app* si possono raccogliere grandi quantità di dati personali relativi all'utente, spesso utilizzate per finalità ulteriori rispetto alle aspettative dell'utente medesimo. La mancanza di trasparenza, e quindi di consapevolezza da parte degli interessati, possono rendere il consenso al trattamento eventualmente manifestato non significativo (informato). Le misure di sicurezza non adeguate, la tendenza a concepire le finalità del trattamento con eccessiva elasticità e l'alto livello di frammentazione tra i diversi attori che operano nel mercato delle applicazioni sono fattori che contribuiscono ad un forte incremento dei rischi per la protezione dei dati.

Il parere, che rivolge raccomandazioni diversificate ai diversi *stakeholder* (sviluppatori delle *app*; proprietari, cd. *app stores*, *etc.*), chiarisce prima di tutto il quadro normativo applicabile, sostanzialmente fondato sulla direttiva 95/46/CE e sulla direttiva cd. *e-Privacy* (2002/58/CE), focalizza l'attenzione sulla necessità che la corretta base giuridica dei trattamenti legati alle *apps* sia il consenso dell'interessato, fornisce chiarimenti, anche ricorrendo ad esempi, sull'applicazione del principio di minimizzazione

dei dati e del principio di finalità, precisa gli obblighi relativi all'adozione di adeguate misure di sicurezza e di trasparenza rispetto agli utenti, si sofferma infine sulle particolari cautele a presidio dei minori nell'utilizzo di *apps*.

Cookies

Il Gruppo si è altresì occupato del tema dei *cookies*, in particolare con l'approvazione del documento di lavoro n. 2/2013 (doc. web n. 2982826) che fornisce indicazioni sulle modalità attraverso le quali i gestori di siti web debbano ottenere il consenso degli utenti per l'uso di tali dispositivi o di altre tecnologie che, analogamente ai *cookies*, consentono il tracciamento della navigazione.

Il Gruppo, prendendo atto che, dall'adozione della direttiva 2002/58/CE emendata nel 2009 e implementata in tutti gli Stati UE, sono state molte le tecniche per ottenere il consenso sviluppate dagli operatori di siti web, sottolinea che tali soggetti sono liberi di adoperare a tal fine i mezzi che siano più consoni alle peculiarità e al *target* del loro sito, purché il consenso raccolto rispetti i requisiti previsti dalla normativa comunitaria. Esso deve quindi fondarsi su una chiara informativa, visibile nello spazio e nel momento in cui il consenso viene richiesto, deve essere ottenuto prima che si dia inizio al trattamento di dati, deve manifestarsi con un'azione positiva o altro comportamento attivo dell'utente dal quale un operatore possa chiaramente desumere la sua volontà di acconsentire al trattamento, deve infine essere effettivamente "libero", garantendo all'utente la possibilità di fornire un consenso "granulare" ed evitando di condizionare l'accesso generale al sito all'accettazione da parte dell'utente di tutti i *cookies*.

Sistemi di misurazione "intelligenti"

Il Gruppo ha inoltre proseguito il suo lavoro sui sistemi di misurazione "intelligenti" nel settore energetico. La Raccomandazione della Commissione 2012/148/EU – il cui intento è quello di offrire agli Stati membri orientamenti sulla progettazione e il funzionamento delle reti e dei sistemi di misurazione intelligenti in modo da garantire il diritto fondamentale alla protezione dei dati personali – ha tra l'altro previsto che gli Stati membri adottino un modello per la valutazione dell'impatto sulla protezione dei dati (cd. *Data Protection Impact Assessment - DPIA Template*). Tale modello, la cui predisposizione è stata affidata ad uno specifico gruppo di esperti della Commissione (EG2), è stato sottoposto due volte al Gruppo Art. 29 che ha fornito indicazioni al riguardo con i due pareri nn. 4/2013 (doc. web n. 2572921) e 7/2013 (doc. web n. 2572931).

Con il primo documento il Gruppo, pur riconoscendo l'importante lavoro svolto dal *team* di esperti, ha giudicato il *template* non sufficientemente maturo soprattutto a causa della mancanza di chiarezza sulla natura e gli obiettivi della *DPIA*, di alcuni difetti metodologici del documento e della carenza di un approccio che tenga conto delle specificità del settore e dei relativi rischi per la protezione dei dati.

Con il secondo parere, il Gruppo ha riconosciuto i considerevoli miglioramenti apportati rispetto al primo modello, specie con riferimento alla precisione del metodo e alla sua fattibilità. Ciononostante, ha indicato ulteriori aspetti suscettibili di riconsiderazione: in particolare, ha raccomandato la predisposizione di un *test* che riguardi casi reali da sottoporre al Gruppo stesso al fine di dimostrare che la valutazione d'impatto costituisca un effettivo miglioramento della protezione dei dati nel settore dei sistemi di misurazione intelligenti, soprattutto riguardo alla *privacy by design* e *by default*, al principio di minimizzazione dei dati, al diritto all'oblio e alla portabilità dei dati, che sono peraltro al centro del pacchetto di riforma attualmente in discussione a livello europeo e che potrebbero dunque divenire in futuro specifici obblighi giuridici.

La *privacy policy* di Google

È proseguita l'importante iniziativa di cooperazione tra le autorità del Gruppo Art. 29 riguardo alla *privacy policy* di Google lanciata il 1° marzo 2012 dalla società di *Mountain View* e che già nell'ottobre del 2012 aveva portato il Gruppo a rivolgere a Google varie raccomandazioni per migliorare le informative, chiarire le modalità di

incrocio dei dati e, più in generale, garantire l'osservanza delle norme e dei principi in materia di prorezione dei dati con meccanismi semplificari di opposizione, raccolta del consenso espresso ai fini della combinazione dei dati per dererminate finalità, limitazione degli incroci di dati relativi ad utenti passivi (doc. web nn. 2375141 e 2375151).

Decorso il periodo previsto per l'adozione di modifiche della *privacy policy* necessarie per assicurare la conformità dei trattamenti alle disposizioni vigenti, i rappresentanti di Google Inc. hanno chiesto un incontro con la *task force* appositamente costituita per la verifica delle regole *privacy* di Google, coordinata dall'Autorità francese e composta anche dalle Autorità per la protezione dei dati di Italia, Germania (Amburgo), Regno Unito, Paesi Bassi e Spagna. A seguito dell'incontro, tenutosi a Parigi il 19 marzo 2013, la società non ha tuttavia adottato alcuna concreta iniziativa nel senso auspicato.

Le menzionate Autorità della *task force* hanno quindi annunciato in contemporanea, il 2 aprile 2013, l'apertura di istruttorie nei confronti di Google Inc. per verificare il rispetto della disciplina sulla protezione dei dati e, in particolare, la conformità dei trattamenti effettuati dalla società di *Mountain View* ai principi di pertinenza, necessità e non eccedenza dei dati trattati, nonché agli obblighi riguardanti l'informativa agli utenti e l'acquisizione del consenso.

All'esito di tali istruttorie, si segnalano allo stato le decisioni dell'Autorità di protezione dei dati olandese che ha ravvisato la violazione della normativa nazionale da parte della *privacy policy* di Google, di quella spagnola che ha risposto alle violazioni perpetrate dal motore di ricerca con una sanzione di €900.000, e dell'Autorità francese che ha sanzionato Google con il massimo finora comminato in Francia (€ 150,000) per non aver provveduto alle necessarie modifiche della sua *privacy policy* (per la parte di competenza dell'Autorità italiana cfr. par. 18.5.2).

Nel corso dell'anno il sottogruppo *technology* ha inoltre esaminato le politiche in materia di protezione dei dati anche di Microsoft. Sotto il coordinamenro delle Autorità di Lussemburgo e Francia, il Gruppo ha dato inizio ad una valutazione congiunta volta a verificare le possibili ripercussioni delle modifiche apportate dalla società a tali *policy* sui diritti degli interessati.

Parere in materia di anonimizzazione

Al Garante è stato affidato il ruolo di correlatore, insieme all'omologa Autorità francese, per la redazione di un patere del Gruppo Art. 29 in materia di anonimizzazione. Il Gruppo ha deciso, anche per chiarire l'ambito di applicazione della disciplina di protezione dei dati che, come noto, si applica ai dati che rendono identificabile una persona, di svolgere un'analisi sull'efficacia e i limiti delle tecniche di anonimizzazione esistenti e disponibili sul mercato. L'analisi ha mostrato che, pur riconoscendosi le potenzialità di tali tecniche che, specie nel caso dell'*open data*, possono rappresentare una strategia utile a mitigare i rischi per gli interessari e a valorizzarne dunque i benefici per gli individui e la società più in generale, diverse pubblicazioni scientifiche e la casistica disponibile mostrano le difficoltà di creare insiemi di dati realmente anonimi.

L'anonimizzazione, risultato di un processo che impedisce l'identificazione dell'interessato in maniera irreversibile, tenuto conto dei mezzi che "ragionevolmente" possono essere impiegati per l'identificazione da parte del titolare del trattamento o di un terzo, costituisce un'operazione ulteriore del trattamento dei dati in questione: l'opinione del Gruppo è che il trattamento ulteriore di dati personali finalizzato alla loro anonimizzazione è compatibile con il trattamento iniziale, purché il risultato finale sia un'effettiva anonimizzazione (de-identificazione irreversibile) nei termini indicati nel parere – tenendo conto del contesto dell'utilizzo dei dati anonimizzati e dei punti di forza e di debolezza delle diverse tecniche utilizzabili per l'anonimizzazione.

Nella sua analisi, il Gruppo non ha mancato di valutare anche la cd. pseudonimizzazione, sottolineando come essa possa sì dirsi un'utile misura di sicurezza che riduce

la diretta correlazione tra il dato e l'identità originale dell'interessato, ma certamente non un metodo in grado di impedire l'identificabilità di un soggetto in modo irreversibile, rimanendo quindi il dato pseudonimizzato pur sempre un "dato personale".

Il messaggio fornito dal Gruppo è che l'anonimizzazione può offrire garanzie per la *privacy* solo nella misura in cui essa sia congegnata in maniera appropriata, valutando caso per caso il contesto di adozione e gli obiettivi di tale tecnica, e tenendo a mente che anche i dati anonimizzati possono presentare rischi per gli interessati, in particolare ove sia ancora possibile ottenere informazioni su di essi attraverso altre fonti di informazioni, siano esse pubbliche o meno. È per questa ragione che è necessaria una valutazione periodica di tali rischi da parte dei titolari del trattamento.

Data breach notification

Il Gruppo ha svolto un approfondimento sulla notificazione in caso di violazione dei dati (cd. *data breach notification*), in particolare rivolto alla individuazione dei criteri di valutazione della severità di tale violazione, con l'obiettivo di fornire ai titolari più chiari parametri sui casi in cui notificare l'evento agli interessati coinvolti (essendo obbligatoria in ogni caso la notifica all'autorità competente, anche alla luce del Regolamento n. 611/2013 adottato in tal senso dalla Commissione europea nel mese di giugno).

Tale attività è stata svolta parallelamente al lavoro dell'*European Union Agency for Network and Information Security* (ENISA) con la quale il Gruppo ha interagito anche attraverso specifici incontri.

Cloud computing

È stata altresì avviata una riflessione sul codice di condotta in materia di *cloud computing* annunciato dalla Commissione con l'obiettivo di individuare uno schema di *governance* del *cloud* valido a livello europeo. Una volta ultimato, tale codice di condotta dovrebbe essere sottoposto al parere del Gruppo Art. 29 in base all'art. 27 della direttiva 95/46/CE.

Altri temi legati alla protezione dei dati nell'ambito delle nuove tecnologie su cui il Gruppo ha avviato una riflessione riguardano la internet delle cose, il cd. *device fingerprinting* (utilizzazione di elementi informativi al fine di consentire l'identificazione univoca ed il tracciamento degli utenti), e il cd. *wearable computing* (dispositivi che possono essere indossati – si pensi al caso di *Google Glass*).

A tal proposito il Gruppo ha sottoscritto una lettera il 18 giugno 2013 (doc. web n. 2985738), di cui è stata promotrice l'Autorità di protezione dei dati canadese, con la quale ha invitato Google ad impegnarsi in un dialogo con le autorità di protezione dei dati dei diversi paesi per chiarire i numerosi profili *privacy* inerenti ai cd. *glasses* (gli occhiali per la cd. realtà "aumentata" progettati dalla società). I Garanti hanno in particolare richiesto chiarimenti in merito alle misure pro *privacy* adottate dagli sviluppatori del prodotto, alle tipologie di dati raccolti da Google attraverso *Glass* e condivise con terze parti, le finalità dei trattamenti in essere, ed eventuali valutazioni di rischio messe in atto da Google.

Altrettanto intensa è stata l'attività del Gruppo in materia di *e-government*.

Parere sulla nuova direttiva *open data*

Subito dopo l'adozione della direttiva 2013/37/UE che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico (cd. direttiva "*open data*"), il Gruppo Art. 29, con il parere n. 6/2013 (doc. web n. 2572941), si è rivolto agli Stati membri per fornire precise indicazioni affinché la trasposizione della stessa negli ordinamenti nazionali avvenga in modo il più possibile omogeneo e tenga conto degli aspetti di protezione dei dati in esso rappresentati.

A differenza della direttiva 2003/98/CE – che si limitava ad armonizzare le condizioni per il riutilizzo delle informazioni del settore pubblico, lasciando tuttavia gli Stati membri liberi di decidere se rendere effettivamente disponibili per il riutilizzo tali informazioni –, la direttiva adottata a giugno 2013 ha introdotto il principio per cui tutte le informazioni detenute dal settore pubblico accessibili in base al diritto nazio-

nale sono riutilizzabili per finalità commerciali e non, a condizione però che tale riutilizzo non pregiudichi le disposizioni in materia di protezione dei dati personali.

Ogniqualvolta un documento pubblico contenga dati personali, infatti, il suo riutilizzo ricade nell'ambito di applicazione della disciplina dettata dalla direttiva 95/46/CE e dalle normative nazionali di recepimento. Alla luce di ciò, il Gruppo, come già nel precedente parere n. 7/2003 reso sul tema (doc. web n. 1609442), ha ricordato che nei casi in cui i soggetti pubblici intendano rendere disponibili per il riutilizzo, oltre a dati aggregati – il cui utilizzo dovrebbe essere sempre privilegiato –, anche dati personali, sarà necessario individuare, in concreto, una solida base giuridica e tenere in considerazione il rispetto dei principi in materia di protezione dei dati personali (e, tra essi, in particolare, i principi di necessità, di proporzionalità e di finalità). Il soggetto pubblico interessato non potrà pertanto limitarsi ad invocare sistematicamente, quale base giuridica per il trattamento, la necessità di rispettare la disciplina sul riutilizzo dei dati pubblici.

Il Gruppo suggerisce, quale buona prassi, l'adozione di misure legislative che specifichino chiaramente e sin dall'inizio quali dati possano essere resi pubblici, per quali finalità e in che misura e a quali condizioni il loro riutilizzo sia possibile. Nell'operare tale valutazione, gli Stati membri saranno tenuti a verificare che la *disclosure* di tali informazioni sia necessaria e proporzionata al legittimo scopo perseguito dalla legge (cfr. Corte europea di giustizia, sentenze del 20 maggio 2003, *Österreichischer Rundfunk*, e del 9 novembre 2010, *Volker und Markus Schecke*).

In questo contesto, cruciale diviene anche il ruolo dei principi di "*privacy by design*" e "*privacy by default*", nonché della valutazione di impatto *privacy* attraverso cui legislatori e soggetti pubblici potranno valutare gli aspetti relativi alla protezione dei dati prima che gli stessi siano resi disponibili per il riutilizzo. Sulla scorta degli esiti di tali valutazioni, i soggetti pubblici interessati potranno identificare misure appropriate per minimizzare i rischi e adottare ogni necessaria misura tecnica, giuridica e organizzativa (quali, ad esempio, specifiche licenze per il riutilizzo o accorgimenti tecnici per evitare la raccolta massiva di informazioni personali) ovvero decidere di non rendere disponibili per il riutilizzo alcuni dati.

Il parere, grazie ad esempi concreti tratti dalle diverse esperienze nazionali, fornisce un quadro di casi in cui la disciplina sul riutilizzo può trovare applicazione e casi di deroga alla stessa e si sofferma sui rischi legati alle tecniche di aggregazione e anonimizzazione di dati, richiamando l'attenzione, in particolare, sulle accresciute possibilità di re-identificazione degli interessati nel nuovo contesto tecnologico.

Lettera su proposta di Regolamento su *e-identity ed e-signature*

Sempre in tema di *e-government*, il Gruppo ha inviato alla Commissaria UE per l'agenda digitale Neelie Kroes una lettera sulla proposta di regolamento sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato unico digitale (COM/2012/0238 final) (doc. web n. 2983174). La proposta in questione mira a creare, nell'ambito dell'Unione, un quadro completo e omogeneo che garantisca transazioni elettroniche sicure e che comprenda l'identificazione, l'autenticazione e la firma elettronica, sostituendo la disciplina dettata dalla direttiva 1999/93/CE che si limita essenzialmente alle firme elettroniche.

Dopo aver suggerito l'utilizzo di definizioni in linea con quelle di comune uso internazionale per termini quali "autenticazione" e "identificazione elettronica", la lettera del Gruppo si sofferma sui rischi di un approccio, quale quello attuale della proposta di regolamento, basato sulla necessità di utilizzare sempre identificatori "univoci" per accedere ai servizi. Tale approccio – a parere del Gruppo – non tiene debitamente conto del fatto che rivelare la propria identità non è sempre necessario e che, in molti casi, sarebbe possibile utilizzare tecnologie o regole maggiormente rispettose del principio di minimizzazione dei dati personali (vedi, ad es., l'utilizzo di sistemi di

identificazione digitali settoriali o sistemi che consentono di verificare solo i requisiti necessari per richiedere un servizio, ad es., l'età). In quest'ottica, il Gruppo suggerisce che il regolamento richiami più spesso la possibilità di utilizzare pseudonimi e riduca la quantità di dati personali che debbano essere resi noti per la verifica di una firma digitale; si auspica anche l'introduzione, nel regolamento, di disposizioni che impediscano che le informazioni personali necessarie per ottenere servizi fiduciari (in caso di autenticazione ad esempio) possano essere utilizzate per profilare gli interessati.

Progetti di ricerca e protezione dei dati

Hanno formato oggetto di valutazione da parte del Gruppo anche gli aspetti relativi alla protezione dei dati personali connessi ai trattamenti effettuati per la gestione di due progetti di ricerca finanziati dalla Commissione europea: il progetto INDECT, relativo all'impatto delle nuove tecnologie per il monitoraggio di comportamenti sospetti sulla rete e nell'ambiente urbano sulla vita privata dei soggetti residenti nell'Unione (doc. web n. 2983082), e il progetto Stork 2.0 (doc. web n. 2983042) che – come il precedente, già esaminato dal Gruppo Art. 29 nel 2011 – riguarda l'interoperabilità a livello europeo dei sistemi di identificazione elettronica.

Con l'occasione, il Gruppo ha concordato di curare un approfondimento sui requisiti richiesti dalla Commissione europea per il finanziamento dei progetti di ricerca in modo da verificare come siano presi in considerazione i profili relativi alla protezione dei dati e alla vita privata. In proposito, sono stati evidenziati i limiti e le difficoltà applicative derivanti dalle attuali condizioni contrattuali predisposte dalla Commissione europea per il finanziamento dei progetti di ricerca nell'ambito del settimo programma quadro. Tali clausole, nella parte in cui richiedono al coordinatore del progetto di presentare una "formale approvazione" da parte delle competenti autorità di protezione dei dati, non risultano coerenti con alcune legislazioni nazionali di attuazione della direttiva 95/46/CE (che, come ad esempio in Italia e Spagna, non prevedono tale tipo di approvazione) e hanno evidenziato l'opportunità di un approccio comune da parte delle autorità di protezione dei dati interessate. Alla luce di ciò, il Gruppo Art. 29 ha preso contatto con la DG Ricerca della Commissione europea che sta lavorando al nuovo programma quadro di investimenti nella ricerca e nell'innovazione per gli anni 2014-2020, *Horizon 2020*, per collaborare alla revisione delle clausole previste per i contratti di finanziamento e delle linee guida sulla *privacy* e sulla protezione dei dati (doc. web n. 2983072).

Law Enforcement

Rilevante è stata inoltre l'attività del Gruppo su proposte sviluppate da parte del *Borders, Travel and Law Enforcement subgroup* (BTLE). Il sottogruppo è nato dall'esigenza di trattare in seno al Gruppo Art. 29 le tematiche connesse al trattamento di dati nel settore di polizia e giustizia (*ex* III Pilastro), dopo l'eliminazione del WPPJ (*Working Party on Police and Justice*) nel corso della *Spring Conference* 2012 in ragione dell'unificazione dei pilastri dell'Unione successiva all'entrata in vigore del Trattato di Lisbona.

Direttiva III pilastro

Il Gruppo ha adottato il Parere n. 1/2013 del 26 febbraio 2013 (doc. web n. 2980389) riguardo alla proposta di direttiva sui trattamenti di dati personali nelle attività giudiziarie e di polizia, formulando specifiche osservazioni e chiedendo maggiori garanzie per quanto riguarda le categorie di interessati, l'esercizio del diritto di accesso, i co-titolari del trattamento ed i poteri delle autorità di protezione dati.

Futuro della supervisione

È stato altresì affrontato il tema della supervisione nel settore del *law enforcement*, in particolare sulla base del documento sul "Futuro della supervisione" sottoposto alla Conferenza di primavera tenutasi a Lisbona (cfr. par. 19.2). Aspetto centrale di tale discussione è stata l'analisi sui punti su cui può registrarsi una convergenza tra le autorità nazionali di protezione dei dati e il Garante europeo (EDPS). In particolare è stato valutato come assicurare coerenza e continuità di controllo per le attività che si svolgono nel settore della cooperazione giudiziaria e di polizia. La

prospettiva del lavoro *in itinere* è di pervenire ad una visione condivisa tra autorità nazionali ed EDPS per poi, in caso positivo, formulare delle proposte per adeguare il quadro normativo. Si è discusso circa l'opportunità di diminuire la pluralità di forme di supervisione oggi esistenti, prevedendo ove possibile un unico sistema di supervisione coordinata tra le autorità nazionali ed il Garante europeo, per tutti quei trattamenti di dati che prevedono la creazione di un *database* centralizzato a livello europeo o scambi analogamente strutturati.

PRISM

Alla luce delle recenti rivelazioni apparse sulla stampa ed ai documenti successivamente resi pubblici in merito al programma PRISM (*Planning Tool for Resource Integration, Synchronization, and Management*) ed altri programmi di raccolta dati a fini di *intelligence*, il Gruppo ha ampiamente dibattuto sulle conseguenze per i cittadini europei di tali attività in vista di una propria presa di posizione – attraverso la predisposizione di un parere in materia di sorveglianza delle comunicazioni elettroniche (previsto per il 2014) – che si soffermi in particolare sul rapporto tra la normativa europea in materia di protezione dati e i programmi di *intelligence* statunitensi. Al riguardo, è stata svolta un'analisi del quadro legale esistente a livello nazionale ed europeo in materia, prendendo in considerazione le basi normative su cui operano i sistemi di supervisione e controllo previsti dagli ordinamenti nazionali. Particolare attenzione è stata rivolta alle richieste della Commissione europea, che ha insistito sulla necessità di maggiore trasparenza nei programmi di *intelligence* e sulla possibilità di un effettivo controllo sulla loro legittimità.

In questa prospettiva è stato quindi redatto ed inviato un questionario alle diverse autorità di protezione dei dati per conoscere le modalità di supervisione sui trattamenti effettuati dai servizi segreti nazionali. È stato affidato al Garante, unitamente all'Autorità ceca, il compito di sviluppare il tema dei sistemi di sorveglianza all'interno dell'Europa e della supervisione dei servizi di sicurezza, al fine di elaborare proposte e raccomandazioni nel parere in preparazione.

In relazione ai menzionati programmi di *intelligence*, il Gruppo Art. 29 ha inoltre manifestato le proprie perplessità alla vicepresidente della Commissione europea Viviane Reding con due lettere, rispettivamente del 7 giugno 2013 (doc. web n. 3019822) e del 13 agosto 2013 (doc. web n. 3019832). In particolare le richieste di chiarimento contenute in tali lettere mirano a comprendere se il programma PRISM implichi il trattamento solamente di dati di cittadini e residenti degli Stati Uniti o se sia invece rivolto anche ai cittadini europei e se l'accesso a tali dati sia mirato o casuale. Il Gruppo ha inoltre comunicato alla vicepresidente Reding l'intenzione di analizzare il quadro legale esistente a livello nazionale ed europeo riguardo all'applicazione della normativa in materia di protezione dati nel contesto dei citati programmi di raccolta dati.

Parere sul concetto di necessità

Sempre in tema di *law enforcement*, il Gruppo ha cominciato a ragionare sulla predisposizione di un parere sul concetto di necessità, calendarizzato per il 2014. Tale parere mira a chiarire i concetti di necessità e proporzionalità – anche alla luce della giurisprudenza della Corte di Strasburgo in relazione all'art. 8 della Convenzione europea per i diritti dell'uomo – nelle misure esistenti predisposte dai legislatori (a più livelli, nazionale o europeo) per rispondere alle esigenze di giustizia e sicurezza.

Accesso ai dati trattati nell'ambito dell'Accordo TFTP2 - programma di controllo delle transazioni finanziarie dei terroristi

In tema di diritti e trasferimento dei dati all'estero, il Gruppo Art. 29 ha poi adottato un modello per l'applicazione uniforme delle procedure relative all'esercizio del diritto di accesso ai dati personali trattati dal Dipartimento del Tesoro statunitense nell'ambito dell'Accordo TFTP2 (Accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (doc. web n. 2613438).

L'Accordo TFTP prevede infatti il diritto di chiunque di accedere ai dati personali che lo riguardano trattati sulla base dell'accordo medesimo e di chiederne la rettifica, la cancellazione o il blocco qualora i medesimi siano inesatti o il trattamento sia in contrasto con l'accordo. Chiunque intenda esercitare tali diritti può presentare una richiesta alla propria autorità nazionale di controllo nell'Unione europea (per l'Italia, il Garante), che agirà da tramite con il Dipartimento del Tesoro statunitense, attraverso apposita modulistica pubblicata sul sito dell'Autorità (cfr. doc. web nn. 2613468, 2613478, 2613488, 2613498).

Border and Travel

Il Gruppo ha esaminato le proposte contenute nello *Smart border package* presentato dalla Commissione e composto di due Proposte di regolamento: la prima relativa all'istituzione di un sistema di ingressi/uscita per cittadini di Paesi terzi che attraversano le frontiere esterne degli Stati membri UE; la seconda all'istituzione di un programma per viaggiatori registrati. Il 6 giugno 2013 ha quindi adottato il Parere n. 5/2013 nel quale, in particolare, si stigmatizzano sia la creazione di un nuovo profilo criminale, quello dei migranti che si trattengono oltre la scadenza del titolo, sia la realizzazione di una ulteriore banca dati centrale oltre a VIS, SIS, Eurodac, nella quale confluirebbero, ai fini della lotta contro l'immigrazione irregolare, i dati personali di chi entra in Europa (doc. web n. 2572931).

Con riferimento al tema dello *screening* anticipato dei passeggeri, è proseguita l'analisi dell'attività dell'*International Air Transport Association* (IATA) e del nuovo modello (NDC) di profilazione degli acquirenti o potenziali acquirenti di biglietti aerei. Il modello NDC realizza un sistema d'individuazione del prezzo del volo basato sulla previa fornitura di una serie di informazioni, anche sensibili, della persona. Grazie al *Dynamic Airline Shopping engine Application Programme Interface* (DAS API) ed alla tecnologia dei messaggi XML, le compagnie aeree potranno fornire un servizio personalizzato agli utenti, basato sullo scambio di dati tra le agenzie di viaggio e gli utenti e le compagnie aeree stesse, ossia sul contenuto della richiesta inoltrata dai viaggiatori o dagli intermediari che agiscono per conto del consumatore finale alle compagnie aeree, tramite messaggio XML. Il menzionato sistema ha suscitato preoccupazioni considerato che il tipo di prodotto, il prezzo e i servizi accessori complementari, verrebbero offerti al cliente in base alle informazioni, tra cui dati personali, riferite a particolari necessità e preferenze, contenute nel predetto messaggio XML.

Protezione dei dati in ambito finanziario

È proseguito il lavoro di approfondimento sui profili di protezione dei dati nel settore finanziario. In particolare il Gruppo Art. 29 si è dedicato all'analisi delle nuove proposte in ambito europeo in materia di contrasto al riciclaggio e al finanziamento del terrorismo e all'impatto che tali disposizioni possono avere sulla protezione dei dati. La linea di tendenza a livello UE è parsa quella di un inasprimento della lotta al riciclaggio e al finanziamento del terrorismo senza però che siano tenuti in dovuta considerazione i diritti delle persone. In tale prospettiva e in linea con le posizioni già assunte dal Gruppo nel Parere n. 14/2011 (doc. web n. 2982816) e dall'EDPS con il Parere del 4 luglio 2013, il Gruppo ha predisposto due lettere, rispettivamente del 4 aprile 2013 (doc. web n. 2982756) e dell'8 novembre 2013 (doc. web n. 2982696), indirizzate al Presidente della Commissione LIBE del Parlamento europeo, con le quali ha manifestato forti preoccupazioni riguardo all'impatto che la proposta di direttiva sulla prevenzione del riciclaggio e la proposta di regolamento sui dati informativi che accompagnano i trasferimenti di fondi potrebbero avere sui diritti delle persone.

Un altro settore di indagine a cui il Gruppo si è dedicato nel corso dell'anno riguarda la profilazione dei clienti nell'ambito creditizio. Attraverso appositi questionari veicolati dalle autorità di protezione dei dati rivolti alle cd. centrali rischi che operano su territorio nazionale, il Gruppo ha svolto un lavoro di approfondimento volto a valutare il livello di adempimento dei principi *privacy* nel settore.

Trasferimento di dati all'estero

Il sistema previsto dagli artt. 25 e 26 della direttiva 95/46/CE per i trasferimenti dei dati verso Paesi terzi e, in particolare, gli strumenti quali il *Safe Harbour*, le clausole contrattuali *standard* e le regole vincolanti d'impresa (BCR) sono stati messi in discussione, nel corso del 2013, a seguito delle notizie relative ai programmi di sorveglianza di massa posti in essere dalle autorità statunitensi (e non solo) a fini di *intelligence* e di sicurezza nazionale e dal sempre maggior utilizzo da parte di soggetti pubblici e privati dei servizi di *cloud computing* (cfr., ad es., lo studio, pubblicato nel 2013 dalla Commissione libertà civili, giustizia e affari interni del Parlamento europeo, "*The US surveillance programmes and their impact on EU citizens' fundamental rights*" (doc. web n. 2983032).

In realtà, *Safe Harbour*, clausole contrattuali *standard* e regole vincolanti d'impresa (BCR) non contengono disposizioni specifiche a tutela degli interessati nel caso di accesso da parte di soggetti pubblici per finalità di sorveglianza (per di più di massa), poiché sono stati creati per governare i flussi transfrontalieri nell'ambito del settore privato e non possono pertanto costituire in alcun modo il fondamento giuridico di un trasferimento di dati per tali altre finalità.

Al riguardo, una riflessione sul tema è stata avviata, in seno al Gruppo, in occasione della decisione di predisporre, nell'ambito del sottogruppo BTLE, il parere relativo alla sorveglianza delle comunicazioni elettroniche a fini di *intelligence* e di sicurezza nazionale (cfr. *supra*) che affronterà, per una parte, anche l'aspetto relativo ai fondamenti normativi vigenti per trasferire dati personali verso gli USA e le condizioni che devono ricorrere alla luce, in particolare, della direttiva 95/46/CE e della Carta dei diritti fondamentali.

BCR e clausole contrattuali *for processor*

Con l'intento invece di rispondere alle sempre più pressanti esigenze di disciplinare i flussi di dati personali nell'ambito di forme di esternalizzazione delle attività di trattamento (quali, ad es., proprio i predetti servizi di *cloud computing*), il Gruppo ha adottato un documento esplicativo delle BCR *for processor* (doc. web n. 2572911) e ha avviato, nell'ambito del sottogruppo *International transfers*, un confronto volto alla predisposizione di un *set* di clausole contrattuali "*for processor*". Tali clausole potranno essere utilizzate – sulla scorta di quanto avviene, ad esempio, nell'ordinamento spagnolo – nei casi in cui un responsabile del trattamento stabilito sul territorio europeo intenda sub-appaltare attività di trattamento di dati personali a soggetti stabiliti in Paesi terzi. Allo stato, anche nel nostro ordinamento, siffatto trasferimento di dati può essere posto in essere dal responsabile del trattamento sulla base di un apposito mandato per la sottoscrizione di clausole contrattuali tipo di cui all'allegato della Decisione della Commissione europea del 5 febbraio 2010, n. 87/2010/UE, conferitogli dal titolare (cfr. Relazione 2012, p. 209 e doc. web n. 2191156).

Per quanto concerne le BCR *for processor* (BCR-P), il documento esplicativo ribadisce che le stesse hanno lo scopo di consentire, nel rispetto delle garanzie previste dalla disciplina di protezione dei dati e senza la necessità di stipulare ogni volta specifici contratti, il trasferimento di dati personali da parte di una società di servizi/responsabile del trattamento situata sul territorio europeo ad una società del medesimo gruppo situata in un Paese terzo e illustra gli elementi essenziali che devono essere contenuti nel contratto generale di servizi (*Service Level Agreement* – SLA) sottoscritto con il cliente/titolare del trattamento e nel resto delle BCR che devono essere allegate al predetto contratto.

Con riferimento agli aspetti procedurali, il documento chiarisce che è la multinazionale interessata a dover presentare l'istanza per l'approvazione delle BCR-P secondo quanto previsto dalla procedura di approvazione da parte delle autorità di protezione dei dati stabilita dal documento di lavoro adottato il 14 aprile 2005 (doc. web n. 1296169) (cfr. Relazione 2005, p. 144), mentre l'autorizzazione nazionale dovrà essere richiesta da ciascun titolare del trattamento che ritenga di avvalersi, in qualità di responsabili del trattamento, di società multinazionali che intendano uti-

lizzare, per trasferimenti di dati verso Paesi terzi, BCR-P già approvate. In tale occasione, copia del contratto generale di servizi dovrà essere presentato alla competente autorità di protezione dei dati al fine di verificare la liceità del trattamento alla luce delle normative nazionali.

Sebbene lo strumento sia stato predisposto dal Gruppo solo a dicembre 2012, già nel 2013 sono state avviate nove procedure europee di approvazione di BCR-P e, tra esse, nel novembre 2013, una ha già concluso il suo *iter* di approvazione.

BCR *for controller*

Per quanto riguarda le BCR *for controller* (BCR-C), lo strumento è già ampiamente conosciuto e utilizzato dalle multinazionali (cfr. Relazioni precedenti), tanto che, nel corso del 2013, sono state avviate ventuno procedure europee di approvazione di BCR-C e sette, iniziate negli anni precedenti, sono state chiuse con il riconoscimento dell'adeguatezza delle disposizioni nelle stesse contenute (per le autorizzazioni nazionali si fa rinvio al par. 13). In tre occasioni il Garante ha operato in qualità di *co-reviewer* insieme all'autorità di protezione dei dati *leader* della procedura (per uno schema esplicativo delle procedure di approvazione, cfr. doc. web n. 2037871), fornendo specifiche indicazioni in ordine a modifiche da apportare nel testo delle BCR proposte dalle società al fine di renderle conformi al quadro normativo europeo.

Adeguatezza e *Referential* BCR/CBPR

Sempre in tema di trasferimento dei dati all'estero, il Gruppo, attraverso il sottogruppo *International transfers*, ha continuato a lavorare ad un documento ("*Referential*") che raccoglie gli elementi comuni tra il sistema BCR europeo e l'analogo sistema delle *Cross Border Privacy Rules*-CBPR adottato in ambito Apec (Cooperazione Economica Asiatico-Pacifica). Il documento, che dovrebbe essere adottato dall'Apec e dal Gruppo nel 2014, intende fornire indicazioni utili per le multinazionali che desiderino adottare regole vincolanti d'impresa che possano ottenere sia un'approvazione europea che una certificazione Apec.

Con riguardo all'attività volta a valutare l'adeguatezza della disciplina nazionale di Paesi terzi, sono inoltre all'attenzione del Gruppo la legge del Québec e la Comunicazione sul funzionamento del *Safe Harbour* (doc. web n. 2983002) con la quale, il 27 novembre 2013, la Commissione (soggetto competente, ai sensi dell'art. 25, comma 6, della direttiva 95/46/CE, a valutare periodicamente l'adeguatezza del regime già riconosciuta con la decisione n. 2000/520/CE), dopo aver illustrato alcuni aspetti critici del sistema, ha fornito tredici raccomandazioni per migliorarne il funzionamento. A quest'ultimo proposito, la Commissione ha chiesto di apportare miglioramenti al regime in tema di trasparenza, di tutela dei diritti degli interessati e di *enforcement* e ha rappresentato la necessità di una maggiore trasparenza da parte delle società iscritte al *Safe Harbour* in ordine ai casi in cui, per motivi di sicurezza nazionale, interesse pubblico o *law enforcement*, le stesse non rispettino i principi del *Safe Harbour*, ricordando che la deroga prevista per la sicurezza nazionale deve essere utilizzata in misura strettamente necessaria e proporzionata. Il riesame dell'intero sistema dovrebbe essere portato a termine dalla Commissione nel 2014 in modo da poter prendere in considerazione le misure di attuazione che le autorità statunitensi intenderanno dare alle raccomandazioni.

Trattamenti effettuati dall'Agenzia mondiale anti-*doping*

Il tema dell'adeguatezza della legge del Québec presenta un peculiare profilo di rilevanza in ragione della circostanza che in tale ordinamento l'Agenzia mondiale anti-*doping* (*World Anti-Doping Agency*-WADA) raccoglie e tratta, attraverso la banca dati ADAMS, i dati personali che gli atleti sono tenuti a comunicare sia direttamente, sia attraverso le federazioni sportive di appartenenza e le competenti organizzazioni nazionali per le finalità anti-*doping*. Nel marzo 2013, nell'ambito della consultazione avviata dall'Agenzia mondiale anti-*doping* in occasione della revisione del codice mondiale e degli *standard* che lo completano, il Gruppo è tornato sull'argomento con una lettera (cfr. doc. web nn. 2983092 e 2983102) con la quale, nel riprendere le conside-

razioni già svolte sul tema nel 2008 e nel 2009 – in occasione dell'adozione di pareri WP 156 (doc. web n. 1619614) e WP 162 (doc. web n. 1620339)–, ha riproposto le proprie perplessità in ordine ad alcuni aspetti della disciplina rimasti invariati rispetto al passato: la funzione del consenso quale presupposto legittimante il trattamento, i lunghi periodi di conservazione dei dati e di pubblicazione delle sanzioni, il rispetto del principio di proporzionalità nel trattamento dei dati relativi ai *whereabouts* (ovvero le informazioni volte a consentire la reperibilità degli atleti ai fini di controlli anti-*doping*), l'uso della banca dati ADAMS e l'assenza di un adeguato quadro giuridico per i flussi transfrontalieri dei dati.

Dal momento che con il nuovo Codice WADA e i relativi *standard*, adottati a novembre 2013, molti dei rilievi mossi dal Gruppo non sono stati recepiti, sono allo stato oggetto di discussione in seno al Gruppo medesimo le iniziative che le autorità di protezione dei dati dovranno porre in essere, anche sul piano nazionale, affinché i trattamenti effettuati dalle competenti organizzazioni nazionali anti-*doping*, ivi compresi i trasferimenti di dati verso la banca dati ADAMS, siano conformi alla disciplina di protezione dei dati.

Supervisione IMI

Con l'entrata in vigore, il 4 dicembre 2012, del Regolamento (UE) n. 1024/2012, è divenuto obbligatorio per la cooperazione amministrativa tra autorità competenti degli Stati membri nel settore del mercato interno l'utilizzo del sistema *Internal Market Information* (IMI). Si tratta di un'applicazione *software* (multilingue ed accessibile tramite internet) sviluppata dalla Commissione in collaborazione con gli Stati membri volta a favorire e accelerare lo scambio transfrontaliero di informazioni, anche personali, e la mutua assistenza previsti in diversi atti dell'Unione (direttiva sui servizi, direttiva sulle qualifiche professionali, direttiva sui diritti dei pazienti, regolamento sul trasporto transfrontaliero professionale di contante in euro, raccomandazione sulla rete per la soluzione dei problemi nel mercato interno-SOLVIT, nonché, sulla base di un progetto pilota, la direttiva sul distacco dei lavoratori).

Trattandosi di un sistema centralizzato, anche in questo caso la Commissione ha ritenuto necessario prevedere uno specifico organismo di supervisione. Il nuovo sistema di supervisione formato dalle autorità competenti a livello nazionale (le autorità di protezione dei dati) e dall'EDPS (cfr. art. 21 del regolamento medesimo) affida a quest'ultimo, come pure accade in altri sistemi, il segretariato del gruppo di supervisione.

L'art. 21 prevede, infatti, che l'autorità o le autorità nazionali di controllo designate in ogni Stato membro e dotate dei poteri di cui all'art. 28 della direttiva 95/46/CE (per l'Italia il Garante) verifichino in modo indipendente la liceità del trattamento dei dati personali da parte dei partecipanti all'IMI del loro Stato membro, garantendo la tutela dei diritti degli interessati. Al controllo da parte delle autorità nazionali si somma quello del Garante europeo della protezione dei dati (EDPS). In particolare, l'EDPS controlla e provvede a garantire che le attività di trattamento dei dati personali della Commissione, nella veste di partecipante all'IMI, si svolgano in conformità al regolamento.

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

Europol: l'attività dell'Autorità di controllo comune [ACC] e del comitato ricorsi

Nel 2013, l'attività dell'ACC Europol, che a marzo ha eletto i nuovi organi (presidente la slovena Natasa Pirc, DP e *Information Commissioner* della Slovenia e vicepresidente Vanna Palumbo del Garante), si è incentrata sull'analisi dell'impatto della proposta presentata dalla Commissione europea di un regolamento che istituisce l'Agenzia dell'Unione europea per la cooperazione e la formazione delle autorità di contrasto (Europol) e abroga le decisioni nn. 2009/371/GAI e 2005/681/GAI del Consiglio.

La proposta, presentata formalmente dalla Commissione europea il 27 marzo 2013 (doc. web n. 2983062), prevede, da un lato, l'assorbimento da parte di Europol delle attività svolte dall'Accademia Europea di Polizia - CEPOL e, dall'altro, un ampliamento dei reati per i quali l'Europol è competente (nonché dei relativi poteri d'indagine), sviluppando anche le sue capacità di fornitore di servizi di comunicazione elettronica (SIENA) e di "*hub*" informativo per i Paesi membri.

Una scelta di fondamentale impatto per l'attività delle autorità di protezione dati è quella operata dalla Commissione riguardo la supervisione dei trattamenti di dati effettuati da Europol, attribuita al Garante europeo della protezione dei dati personali, come anche la competenza in materia di esercizio del diritto di accesso degli interessati e la decisione in merito ad eventuali ricorsi da questi presentati. Il modello di supervisione con al centro l'EDPS viene quindi progressivamente esteso dalla Commissione ad ogni nuovo strumento legislativo (anche le proposte concernenti Eurojust ed il procuratore europeo (EPPO) sono sulla stessa linea). I Garanti europei hanno discusso nella conferenza di primavera il tema, adottando una risoluzione abbastanza critica e preoccupata (v. par. 19.2) (doc. web n. 2980604).

L'Autorità di controllo comune Europol ha a sua volta adottato due pareri, il primo nel giugno ed il secondo nell'ottobre 2013, sulla proposta di regolamento. Con il primo parere (doc. web n. 2983184), anche sulla scorta della richiamata risoluzione dei Garanti europei, ha rilevato che l'ampliamento del ruolo e delle responsabilità di Europol avverrebbe a scapito della certezza giuridica necessaria a garantire la correttezza e controllabilità del suo operato, in particolare, nella misura in cui gli verrebbero attribuiti un compito di coordinamento nelle indagini e una competenza non più per "grave reato" ("*serious crime*") ma sulla base del più indeterminato criterio delle "forme di criminalità che ledono un interesse comune oggetto di una politica dell'Unione", nonché un ulteriore e non disciplinato ruolo di *provider* di servizi di comunicazione elettronica. Il parere si sofferma inoltre sull'effetto di tali cambiamenti sulle modalità di trattamento dei dati e quindi sulla struttura dei sistemi informatici finora creati (e, come noto, controllati con cadenza annuale dall'ACC attraverso il suo gruppo ispezioni) e sull'impatto degli stessi sulla supervisione dei trattamenti di dati personali effettuati.

Un secondo, più analitico parere è stato adottato il 9 ottobre 2013 (doc. web n. 2983132). Con lo stesso si evidenziano le lacune e le contraddizioni del testo proposto dalla Commissione rispetto alle finalità dichiarate e il conseguente rischio di una riduzione delle garanzie previste in materia di protezione dei dati rispetto a quelle della decisione n. 2009/371/GAI attualmente in vigore. Gran parte dei rilievi si fondano sull'esperienza acquisita dall'ACC nell'espletamento dei suoi compiti di controllo della legittimità dei trattamenti di dati effettuati da Europol, in particolare in occasione dell'ispezioni svolte in *loco*. Il parere è stato inviato al Consiglio, che ha in discussione il testo della proposta di regolamento, ed al Parlamento europeo.

L'ACC ha inoltre svolto, come di consueto, il controllo annuale sui trattamenti di dati effettuati da Europol e ha approvato il rapporto sull'attività ispettiva svolta. Il Garante ha partecipato con un proprio esperto all'ispezione svolta nel 2013 che ha incluso anche la verifica delle modalità con cui Europol effettua i trattamenti di dati in relazione ai compiti affidati dall'Accordo USA-UE sul TFTP (l'Accordo sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi).

Rispetto a tale tipologia di trattamento, l'ACC ha reso pubblica intanto, come era già avvenuto per l'anno precedente, una breve sintesi che illustra gli esiti della terza (ed ultima specifica) ispezione condotta nel novembre 2012 (doc. web n. 2983142) e ha accolto la richiesta dell'Ombudsman europeo di poter accedere alla parte secretata del rapporto sull'ispezione.

Per quanto riguarda l'attività dei sottogruppi, ci sono stati due incontri con i rappresentanti di Europol presso la sede dell'Aja per continuare l'analisi delle modalità di fornitura ed uso della rete per lo scambio di informazioni SIENA (che collega Europol alle autorità preposte ad attività di contrasto negli Stati membri e ad altri partner). Anche sulla scorta di tali incontri, l'ACC ha adottato, a dicembre, uno specifico parere sul tema. Altri pareri hanno riguardato due progetti di accordi operativi con Serbia e Albania (doc. web nn. 2983122 e 2983112) e le future attività di Europol (doc. web n. 2983162).

L'ACC ha adottato inoltre il rapporto sulle attività svolte nel quadriennio 2008-2012 (doc. web n. 2996478) e un rapporto sul funzionamento delle Unità nazionali Europol con particolare riguardo alla fase di introduzione dei dati nei sistemi Europol o di loro invio (doc. web n. 2983152). Quest'ultimo rapporto, traendo le conclusioni dalle risposte pervenute ad un questionario predisposto nel 2012, evidenzia la non completa armonizzazione del ruolo e delle responsabilità attribuiti, nei diversi Stati membri, alle Unità nazionali e formula alcune raccomandazioni al riguardo.

Il Sistema Informativo Schengen: l'attività dell'Autorità di controllo comune [ACC] Schengen e il nuovo Gruppo di coordinamento della supervisione SIS II

Dal 9 aprile 2013 è attivo il Sistema d'informazione Schengen di seconda generazione (SIS II). Dalla stessa data, pertanto, è cambiata la base giuridica per il trattamento dei dati personali effettuato nel sistema – non più disciplinato dalla Convenzione "Schengen" (integrata nel quadro istituzionale e giuridico dell'Unione europea nel 1999) ma dal Regolamento (CE) n. 1987/2006 di Parlamento europeo e Consiglio del 20 dicembre 2006 e dalla decisione n. 2007/533/GAI del Consiglio del 12 giugno 2007 che istituiscono e disciplinano il SIS II (doc. web nn. 2983012 e 2982882) – e l'Autorità comune di controllo Schengen ha concluso la propria attività di supervisione e controllo.

Il sistema SIS II, operativo dal 1995, ha lo scopo di aumentare la sicurezza e di facilitare la libera circolazione nello spazio Schengen, permettendo alle autorità nazionali doganali, di polizia e di controllo delle frontiere di scambiarsi agevolmente informazioni. Il Sistema contiene infatti segnalazioni sulle persone scomparse (soprattutto minori) e informazioni su determinati beni (quali banconote, automobili, furgoni, armi da fuoco e documenti di identità) che potrebbero essere stati rubati, sottratti o smarriti. È dotato di funzioni avanzate, come la possibilità di inserire dati biometrici (impronte digitali e fotografie), nuovi tipi di segnalazioni (aeromobili, natanti, *container* e mezzi di pagamento rubati) o la possibilità di collegare segnalazioni diverse (ad es., una segnalazione su una persona e su un veicolo). Il SIS II contiene copie dei mandati d'arresto europei collegati direttamente a segnalazioni per l'arresto a fini di consegna o di estradizione.

L'accesso al sistema è limitato alle autorità nazionali giudiziarie, doganali e di polizia e a quelle competenti per il controllo delle frontiere, i visti e i certificati di immatricolazione per veicoli. Come per il SIS I, chiunque ha il diritto di accedere ai dati che lo riguardano inseriti nel nuovo sistema può chiedere all'autorità nazionale competente di rettificare o cancellare i propri dati personali. Inoltre, chiunque può agire in giudizio per accedere alle informazioni, rettificarle, cancellarle o per ottenere un indennizzo nel caso di segnalazione che lo riguardi inserita illecitamente. È anche previsto che, almeno ogni 4 anni, si proceda ad una verifica della conformità dei trattamenti effettuati.

L'entrata in funzione del SIS II è stata accompagnata, come previsto dalle nuove basi giuridiche, da una campagna informativa in tutti i Paesi secondo modelli *standard* plurilingue, predisposti dalla Commissione che dovrebbero essere distribuiti sia nei punti di frontiera sia sul territorio.

In questo quadro di cambiamento, l'ACC Schengen – di cui sono stati fatti circolare i rapporti di attività (2008 - aprile 2013, doc. web n. 2982892) – ha tenuto la sua

ultima riunione nella pienezza dei poteri nel marzo 2013, adottando il rapporto relativo ai lavori di verifica sull'inserimento nel sistema delle segnalazioni *ex* art. 95 della Convenzione (mandato di arresto europeo) e lasciando al Gruppo di coordinamento della supervisione SIS II – cui ha passato il testimone – il compito di portare a termine le attività avviate in relazione all'esercizio del diritto di accesso e ai criteri per l'introduzione nel sistema delle segnalazioni relative a veicoli rubati.

Il Gruppo di coordinamento – che si è riunito, per la prima volta, nel giugno 2013, adottando il regolamento interno ed eleggendo, quale presidente, Clara Guerra, dell'Autorità di protezione dei dati portoghese, e, come vicepresidente, David Cauchi, del Garante maltese – è stato informato, da rappresentanti della DG Affari interni della Commissione europea e dell'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (EU-LISA), su modi e forme del passaggio dal SIS I al SIS II, avvenuto senza problemi dal punto di visto informatico ed operativo. Il menzionato Gruppo ha poi costituito un sottogruppo tecnico incaricato, tra l'altro, di seguire gli sviluppi di un'indagine avviata su un grave caso di *data breach* al SIRENE danese, avvenuto a seguito di un attacco di *hacker* e reso noto nel giugno 2013. Proprio alla luce di tale evento, gli Stati Schengen sono stati chiamati, attraverso la compilazione di un questionario, a svolgere un *self-assessment* dei sistemi nazionali e della sicurezza della trasmissione dei dati, anche tenendo conto di eventuali forme di *outsourcing*/subcontratto nella gestione operativa degli stessi.

Il Sistema informativo doganale (SID): ACC Dogane e Gruppo di coordinamento della supervisione SID

L'ACC Dogane e il Gruppo di coordinamento della supervisione del Sistema informativo doganale (SID) si riuniscono normalmente insieme in quanto condividono la supervisione sullo stesso *database* in cui sono trattati dati di cooperazione doganale relativi agli *ex* primo e terzo pilastro.

L'ACC Dogane ha proseguito la sua attività adottando il rapporto di attività fino a dicembre 2013, il nuovo programma di lavoro e una lettera sull'accesso al SID attraverso un singolo punto di contatto. È stata inoltre messa a punto una *brochure* informativa, dal titolo "Guida alle vostre responsabilità", rivolta alle autorità doganali ed alle altre autorità che hanno accesso al SID, che fornisce indicazioni per i casi in cui i dati inseriti nel sistema doganale comune SID non siano accurati o leciti (art. 13 della decisione SID 2009/917 ed art. 8 (2) della decisione quadro protezione dati 2008/977).

Il Gruppo di coordinamento della supervisione SID ha confermato per un secondo ed ultimo mandato Presidente e Vicepresidente. Sono in corso attività relative alla verifica della lista delle autorità che possono avere accesso al SID (comunicate da ciascuno Stato membro alla Commissione europea) e verrà esaminata, al fine di predisporre un parere, la proposta di modifica del Regolamento presentata a novembre 2013 dalla Commissione europea e l'ulteriore proposta di modifica della supervisione del sistema (doc. web n. 2983022).

Il Sistema Informativo Visti (VIS): Gruppo di coordinamento della supervisione VIS

Il Gruppo di coordinamento della supervisione VIS, che ha approvato il regolamento interno ed ha proceduto alla elezione del Presidente (Peter Hustinx, EDPS) e del Vicepresidente (Vanna Palumbo, del Garante), ha conferito lo *status* di osservatori, su loro richiesta, ad Irlanda e Regno Unito, Paesi non partecipanti alla cooperazione Schengen ed alle misure dell'Unione adottate sulla base di questa (in sostanza, la quasi totalità delle attività in materia di asilo ed immigrazione, controllo delle frontiere *etc.*).

È stato discusso e adottato il programma di attività per il biennio 2013-2014, anche con riferimento all'attività di supervisione. Tale attività riguarderà non solo la parte centrale del sistema, posta sotto la responsabilità operativa dell'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (EU-LISA), ma anche le parti nazionali del VIS; oggetto di verifica sarà anche il modo in cui le forze dell'or-

dine hanno accesso ai dati secondo quanto previsto dalla decisione 2008/633/GAI. Sul tema dello sviluppo di possibili *standard* per effettuare le ispezioni, sia a livello nazionale sia congiuntamente, ad esempio nei Paesi in cui gli uffici diplomatici di uno Stato membro emettono visti anche per altri Stati UE, il Gruppo sta valutando se e quali *standard* internazionali possono essere applicati, cercando di mantenere la sinergia con il lavoro già fatto dal Gruppo Eurodac (che potrà essere adattato alle specificità delle verifiche sul VIS). Il Gruppo ha poi esaminato le implicazioni per la protezione dei dati del sistema, in particolare per quanto riguarda i responsabili del trattamento (*sub contractors*). Al riguardo è stato deciso di istituire un piccolo sottogruppo che approfondirà il tema, anche basandosi sulle ispezioni nelle sedi di tali soggetti già effettuate da alcune DPA.

Quanto alle attività del prossimo biennio, l'attenzione del Gruppo si focalizzerà oltre che sugli aspetti sopra indicati, sui soggetti che possono accedere al sistema, sulle modalità di esercizio del diritto di accesso, rettifica, *etc.*, nonché sulle modalità di accesso delle LEAs al sistema.

Gruppo di supervisione Eurodac

L'attenzione del Gruppo è stata in massima parte rivolta ad un'analisi degli sviluppi derivanti dall'adozione, il 26 giugno 2013, della proposta di rifusione (cd. *recast*) del regolamento Eurodac (regolamento (UE) n. 603/2013, doc. web n. 2983052) che, tra l'altro, renderà possibile l'accesso ai dati contenuti nella banca dati Eurodac da parte delle forze di polizia, con conseguenti modifiche all'architettura del sistema (quali la possibilità di consultare il *database*, ai fini di polizia, anche a partire da frammenti di impronta ritrovati sulla scena del crimine).

Tenendo conto della sensibilità del trattamento dei dati di richiedenti asilo, l'accesso agli stessi sarà consentito a polizia ed inquirenti e ad Europol solo qualora dall'interrogazione delle banche dati di polizia nazionali o del VIS non emergano già riscontri: garanzie, queste, non ritenute tuttavia sufficienti dai Garanti che hanno eccepito, oltre alla mancata dimostrazione della necessità e proporzionalità della misura, la finalità "incompatibile" dell'utilizzo dei dati previsto dal regolamento rispetto alla finalità della loro raccolta.

Alla luce di ciò, il Gruppo EURODAC ha deciso di focalizzare anche le prossime attività sulla valutazione del nuovo regolamento, con lo scopo di influenzare la definizione dell'architettura del sistema, in particolare introducendo delle funzionalità che consentano di registrare separatamente gli accessi delle forze di polizia da quelli delle autorità competenti per le procedure di asilo. Ciò considerato anche che dalla data di adozione del testo a quella dell'entrata in funzione del sistema nella nuova forma intercorreranno due anni (il regolamento entrerà in vigore infatti il 20 luglio 2015).

Sulla scorta di lavori pilota svolti da alcune delegazioni, il Gruppo ha inoltre messo a punto un piano di ispezione standardizzato, da utilizzare a livello nazionale per l'attività di supervisione e controllo attribuita dal regolamento Eurodac.

A maggio 2013, alla luce delle risposte fornite dalle competenti autorità nazionali ad un questionario volto a verificare le modalità utilizzate per la raccolta delle impronte digitali dei richiedenti asilo e le conseguenze in caso di impronte illeggibili (cfr. anche Relazione 2012, p. 294), il Gruppo ha approvato il rapporto sull'ispezione coordinata sulle impronte illeggibili con cui si raccomanda l'adozione di procedure uniformi nei diversi Stati membri e l'introduzione da parte del legislatore europeo di una specifica disposizione che preveda espressamente che il semplice possesso di impronte illeggibili non determini effetti negativi sulla procedura di riconoscimento dello *status* di rifugiato (doc. web n. 2985748).

19.5. *La partecipazione ad altri comitati e gruppi di lavoro*

IWGDPT: il Gruppo di Berlino - *International Working Group on Data Protection in Telecommunication*

L'Autorità ha proseguito la sua partecipazione all'*International Working Group on Data Protection in Telecommunication*, cd. Gruppo di Berlino, che nel corso del 2013 si è riunito come d'uso due volte (a Praga in primavera ed a Berlino a fine estate).

In qualità di relatore, l'Autorità ha lavorato all'adozione del documento sulla pubblicazione di dati personali sul web, adottato nella riunione di Praga, che, affrontando il tema da un punto di vista tecnologico, ha individuato metodologie e soluzioni per realizzare un efficace esercizio del diritto all'oblio. Il documento ha fornito inoltre precise raccomandazioni per ciascuno degli attori coinvolti (*webmaster*, motori di ricerca) e buone pratiche tecnologiche, evidenziando che il raggiungimento di un'effettiva tutela dei diritti degli interessati richiede un approccio multilaterale fondato sull'azione coordinata dei vari *stakeholder* (doc. web n. 2982786).

Nel documento di lavoro sul *web tracking* adottato nella stessa riunione ed essenzialmente indirizzato ai fornitori di siti web, sviluppatori di *software* e di tecnologie che consentono il tracciamento degli utenti della rete, il Gruppo ha fornito specifiche raccomandazioni volte a garantire trasparenza e controllo da parte degli interessati. In particolare, occorre valorizzare e attuare anche nel contesto del *tracking*, il rispetto della finalità del trattamento evitando che pratiche di condivisione dei dati rendano possibile il loro utilizzo in un contesto diverso da quello della raccolta e all'insaputa dell'interessato (doc. web n. 2982776).

La riunione di Berlino ha invece portato all'adozione di due ulteriori documenti, rispettivamente sulla segretezza delle telecomunicazioni e sulla sorveglianza aerea.

Il primo, in risposta ai recenti fatti legati alla sorveglianza delle comunicazioni svolta su scala mondiale dalle autorità di *law enforcement* e dai servizi segreti di alcuni Paesi, esorta i governi a: riconoscere la segretezza delle comunicazioni come una parte essenziale del diritto alla vita privata e a rafforzarla anche attraverso il suo riconoscimento, tra i diritti fondamentali, in una convenzione internazionale; predisporre *standard* internazionali volti a limitare l'accesso, da parte delle autorità pubbliche, ai dati personali conservati dai fornitori di servizi internet; incoraggiare l'impiego di forme sicure di comunicazione tra i cittadini e assicurare un controllo indipendente ed effettivo riguardo alle attività di sorveglianza svolte dalle autorità di polizia e di *intelligence* o, per loro conto, da soggetti privati (doc. web n. 2982796).

Nel documento di lavoro sulla sorveglianza aerea, il Gruppo ha inteso sottolineare che la particolare intrusività e invisibilità dell'impiego di nuovi dispositivi quali i droni, unita al fatto che essi portano a una sorveglianza indiscriminata e potenzialmente continua sulle persone, rende ineludibile l'implementazione di misure specifiche: prima di tutto garantire che l'impiego della sorveglianza aerea sia limitata a specifiche finalità, ad esempio la ricerca di persone scomparse; far sì che l'impiego di immagini raccolte attraverso i droni dalle autorità pubbliche sia soggetto a mandato giudiziario; assicurare la massima pubblicità di tali impieghi; limitare la sorveglianza ad aree il più possibile circoscritte; garantire controlli stringenti sull'utilizzo delle informazioni raccolte e sull'accesso a tali dati. Misure volte, cioè, ad assicurare un giusto bilanciamento tra gli interessi pubblici perseguiti e la legittima aspettativa di *privacy* delle persone (doc. web n. 2982806).

Nel corso dell'anno il Gruppo ha altresì deciso di affrontare il tema del cd. *wearable computing*, ossia dei dispositivi che possono essere indossati e che possono dare luogo a forme di sorveglianza indiscriminata e nascosta, e di avviare un'attività ricognitiva sul cd. *bring your own device* (BYOD), uno schema di cooperazione tra individui che mettono in condivisione i propri terminali e applicazioni all'interno di una rete (in diversi contesti: all'interno di pubblica amministrazione, di una sala

conferenza, di un esercizio commerciale, *etc.*). Da esso possono infatti nascere problemi di sicurezza dei dati ad esempio legati all'uso promiscuo dei terminali negli ambiti domestico e lavorativo o alla condivisione degli stessi da più persone, nonché forme di sorveglianza suscettibili di ricadere nell'ambito di applicazione della disciplina sulla protezione dei dati personali.

Data retention - Expert Group

Con decisione C(2013)2144 del 18 aprile 2013, la Commissione europea ha deciso di istituire un nuovo gruppo di esperti – *Data Retention Expert Group* – che, in continuità con il lavoro svolto dal precedente gruppo il cui mandato è terminato nel 2012, ha ricevuto l'incarico di approfondire gli aspetti legati alla direttiva 2006/24/CE (cd. *data retention*, ovvero conservazione dei dati) ed in particolare di predisporre *best practice* sulla conservazione dei dati relativi alle comunicazioni elettroniche a fini investigativi e per la persecuzione di gravi reati. Il Gruppo è formato da rappresentanti delle società fornitrici di servizi di comunicazione elettronica, da rappresentanti delle forze dell'ordine e di polizia nonché da rappresentanti delle Autorità di protezione dei dati. Il Garante partecipa all'attività del *Data Retention Expert Group*. Il Gruppo, sui cui lavori hanno avuto peso le conclusioni presentate dall'avvocato generale della Corte di Giustizia dell'Unione europea il 12 dicembre 2013 riguardo alla direttiva *data retention* (Causa C-293/12), nonché la prospettiva di una imminente decisione della stessa Corte di Giustizia in merito (poi intervenuta, come si è detto al par. 10.2), sta comunque continuando l'attività di predisposizione di un manuale sulle buone prassi in materia di conservazione dei dati che dovrebbe venire alla luce nel corso del 2014.

Consiglio d'Europa

Anche il 2013 è stato caratterizzato dal lavoro di revisione della Convenzione n. 108/1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

Parallelamente al pacchetto di riforma in discussione al livello UE, anche il Consiglio d'Europa (CoE) ha infatti ritenuto necessario rivedere tale Convenzione alla luce delle tante novità emerse negli ultimi decenni, sia con riferimento allo sviluppo tecnologico che alla crescente globalizzazione.

La discussione in seno al CoE si è peraltro svolta con l'intento di assicurare un quadro di principi coerenti con il progetto di revisione degli strumenti di protezione dei dati in discussione a livello UE.

Come anticipato, il T-PD, Comitato della Convenzione a cui il Garante partecipa da anni, anche nella sua composizione ristretta (T-PD Bureau), aveva concluso nel 2012 il lavoro tecnico relativo alla modernizzazione della 108, con l'adozione, in occasione della sua 29ma plenaria, di un documento finale contenente le proposte di revisione della Convenzione (cfr. Relazione 2012, p. 298, doc. web n. 2375191).

Con l'adozione del menzionato documento da parte del T-PD, che ha comunque proseguito la sua riflessione sulla revisione della Convenzione n. 108, impegnandosi nella redazione del *Memorandum* esplicativo che accompagnerà il progetto, si è aperta la fase "politica" della modernizzazione di tale settore alla quale l'Autorità ha continuato a partecipare.

Il Comitato dei Ministri del Consiglio d'Europa il 10 luglio 2013 ha infatti deciso l'istituzione di un Comitato *ad hoc* (CAHDATA) composto dai rappresentanti degli Stati membri del Consiglio d'Europa, di altre Parti che hanno aderito alla Convenzione, e da Stati che non fanno parte del CoE, con il compito di finalizzare il processo di revisione e negoziare formalmente un Protocollo emendativo alla Convenzione n. 108.

Il Segretario generale del Garante è stato designato rappresentante per l'Italia all'interno del CAHDATA e ha dunque preso parte alla prima riunione del Comitato che si è tenuta a Strasburgo il 12-14 novembre 2013.

In tale incontro, durante il quale sono stati eletti il rappresentante irlandese e la rappresentante svizzera, rispettivamente alla Presidenza e alla Vicepresidenza del

Comitato, è emerso un generale plauso per il lavoro svolto dal T-PD le cui proposte di modifica alla Convenzione hanno costituito la base di discussione del CAHDATA. È altresì emersa la necessità di riflettere sul giusto equilibrio che la nuova Convenzione dovrà garantire tra l'esigenza di mantenere un'impostazione coerente con il quadro comunitario e quella di preservare la vocazione universale della 108, fondata su principi di carattere generale.

Il CAHDATA ha dunque effettuato una prima lettura "esplorativa" del testo proposto dal T-PD che, come illustrato nella Relazione 2012, pur mantenendo il carattere trasversale della Convenzione (applicabile sia al settore privato sia a quello pubblico) tecnologicamente neutro e fondato su principi di carattere generale, ha innovato su diversi punti salienti della stessa.

Parallelamente alla discussione sulla Convenzione n. 108, il T-PD ha proseguito il suo lavoro sul processo di revisione delle raccomandazioni del CoE, in particolare della Raccomandazione (89)2 sulla protezione dei dati in ambito lavorativo e della Raccomandazione (87)15 sull'utilizzo dei dati a carattere personale nel settore della polizia. È stata inoltre avviata una riflessione sulla opportunità di rivedere anche la Raccomandazione (97)5 sui dati sanitari, alla luce delle innumerevoli novità tecnologiche nel settore medico, in particolare con riferimento al Fse, alla telemedicina, all'impiego di RFID e di applicativi ("*app*").

Il T-PD ha inoltre portato avanti la riflessione sulla protezione dei dati biometrici dalla quale è emersa l'opportunità di proseguire il lavoro già svolto, ampliando il *Progress Report* del 2005 in modo da dar conto del mutato contesto tecnologico degli ultimi anni, ed in particolare tenendo conto delle tecniche biometriche di seconda generazione che consentono classificazioni automatizzate di individui anche all'insaputa degli stessi interessati.

L'Autorità ha continuato a partecipare ai lavori del WPISP (*Working Party on Information Security and Privacy*) dell'Ocse. Nel 2013 il Garante, già membro del Gruppo e del *Bureau* del WPISP, è stato riconfermato nel *Bureau* del Gruppo anche per il 2014. **OCSE**

Attività centrale del lavoro del WPISP è stata la revisione delle linee guida *privacy* dell'Ocse del 1980 (*Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*) che ha portato all'adozione del documento finale da parte del Consiglio Ocse, avvenuta l'11 luglio 2013 (doc. web n. 2629667). Si è giunti così all'approvazione delle *Revised Privacy Guidelines* attraverso una vivace e contrastata discussione durata diversi mesi, alla quale il Garante ha attivamente contribuito affinché il nuovo testo mantenesse un adeguato livello di tutela dei diritti delle persone anche alla luce del quadro europeo di protezione dei dati.

Al centro delle linee guida aggiornate emergono, tra gli altri, due temi. Il primo è un *focus* sulla realizzazione pratica della protezione della *privacy*, attraverso un approccio fondato sulla gestione del rischio. Il secondo riguarda la necessità di affrontare la dimensione globale della protezione dei dati personali attraverso una migliore interoperabilità.

L'attività del WPISP degli ultimi mesi del 2013 si è concentrata sull'esigenza di implementare le linee guida *privacy*, anche attraverso: la diffusione e promozione del testo; lo sviluppo di programmi di *privacy management* (che rientrano nel quadro degli obblighi di *accountability* che ricadono sui titolari del trattamento); l'attuazione della cd. *data security breach notification*; l'elaborazione di strategie nazionali di interoperabilità globale in materia di protezione dei dati personali.

Quanto al tema della *cybersecurity*, il WPISP ha proseguito i lavori del Gruppo di esperti (costituito nel 2012) sulla Revisione delle linee guida sicurezza Ocse del 2002 (*Guidelines for the security of Information Systems and Networks).* Il lavoro è confluito

in un Rapporto in cui è stata evidenziata la necessità di coinvolgere altri esperti per portare avanti la più amplia consultazione possibile per una revisione complessa che deve dare un messaggio importante su un nuovo approccio "in positivo" sulla sicurezza intesa come mezzo per la crescita economica e la prosperità e non solo come "sicurezza da" in termini di difesa da attacchi esterni. A tal fine, è stata condivisa la necessità di trasparenza e di controllo da parte degli utenti. Quanto più gli utenti sono messi in condizione di comprendere (attraverso delle linee guida chiare ed *user-friendly*) e controllare la sicurezza della rete, tanto più la sicurezza sarà positiva e diventerà fattore di crescita globale.

Un altro settore al quale il WPISP nel corso del 2013 ha dedicato attenzione è quello relativo al valore economico dei dati e al ruolo degli stessi nel promuovere la crescita economica e il benessere globale, con particolare riferimento ai cambiamenti tecnologici e organizzativi rappresentati dai *big data* e alle relative analisi di impatto economico. Sono stati affrontati dal WPISP gli argomenti di *privacy* emergenti nella cosiddetta *data driven economy*. La nozione di *trust*, intesa come fiducia nella tecnica e nell'etica dei titolari del trattamento dei dati, è stata molto dibattuta nel corso dell'anno e sempre più associata al benessere economico e alla prosperità. Per la maggior parte delle delegazioni del Gruppo la nozione di *trust* sta diventando un cappello sotto il quale far rientrare tutto ciò che può considerarsi in altri termini *accountability* e affidabilità nella gestione dei dati personali. In ogni caso, il lavoro sulla "*security in a data driven economy*" resta un lavoro *in itinere* che per ora si limita ad introdurre solo delle riflessioni preliminari.

Infine, si segnala che nel dicembre 2013 è stato modificato il nominativo del Gruppo per la necessità condivisa di aggiornare – in relazione ai cambiamenti tecnologici in atto – la forma e il mandato del WPISP (costituito nel lontano 1995). Il cambiamento comporta il passaggio dell'acronimo da WPISP in *WPSP in the Digital economy*. A livello sostanziale, il mandato del lavoro del Gruppo sarà più contenuto e concentrato nello sviluppo di "principi" di *policies* (e non più *policies* in senso largo), linee guida e *best practices* con particolare riferimento alle aeree in cui vi è un crescente bisogno di cooperazione transfrontaliera.

Accountability Project

Nel 2013 si è concluso il lavoro dell'*accountability project*, iniziato nel 2009 e illustrato nelle precedenti relazioni annuali.

La quinta ed ultima fase del progetto, che ha visto riunirsi gli esperti due volte, rispettivamente in Europa (Varsavia) e in Canada (Toronto), si è incentrata sulla ricerca di un consenso sugli aspetti di rischio per i diritti e le libertà fondamentali delle persone in caso di trattamento illecito di dati personali da parte di titolari del trattamento non *accountable*. I partecipanti hanno condiviso e discusso un possibile elenco di rischi frutto del confronto avutosi nel corso delle riunioni della fase IV del progetto e dei vari contributi fatti pervenire dagli esperti.

Anche a causa della difficoltà di trovare, sia a livello internazionale che europeo, definizioni *ad hoc* e parametri condivisi sui rischi e i danni tangibili ed intangibili (ad es., alla reputazione o alla dignità) per i singoli individui derivanti dal trattamento dei dati da parte delle organizzazioni, è stato ritenuto necessario un approccio basato sulla valutazione dei rischi caso per caso. Gli esperti hanno analizzato il rapporto *accountability*/rischi, in particolare enfatizzando la necessità di un forte canale di comunicazione tra titolare e interessato (per incrementare il livello di consapevolezza sui trattamenti e di riduzione dei rischi, nonché la fiducia tra le parti coinvolte), di adeguate misure di sicurezza, di trasparenza sulle finalità del trattamento, di *policy* chiare e condivise. Tutti questi elementi devono essere finalizzati al raggiungimento di un più elevato livello di responsabilità "misurabile" (anche da parte dell'interessato). È emersa, inoltre, la necessità di avviare un dibattito sul tema della fiducia/*trust* come bene pub-

blico da tutelare con adeguati strumenti tecnico-normativi. L'*accountability* è uno degli strumenti che si prestano a questo scopo e dovrà essere implementata ad ogni livello (realtà economiche, pubbliche amministrazioni, Stati). Infine, è stato affrontato il tema della cd. scalabilità, ossia della necessità di disporre di strumenti in grado di gestire le varie fasi quantitative di "misurazione" dei parametri necessari al raggiungimento degli obiettivi di *accountability*. Occorre infatti evidenziare che l'*accountability*, considerata come una forma di responsabilità misurabile, richiederà a realtà economiche o amministrazioni (anche di piccole o piccolissime dimensioni) di trattare grandi quantitativi di dati relativi a interessati, anche in contesti sovranazionali. L'industria, dal canto suo, dovrà fornire strumenti efficaci e "usabili" per consentire queste operazioni anche a titolari non particolarmente forniti di competenze specialistiche, o sofisticati strumenti tecnologici.

Cooperazione internazionale GPEN, IECWG, *PHAEDRA project*

Nell'ambito della Conferenza internazionale (cfr. par. 19.2), si è deciso di rafforzare l'attività del *Global Privacy Enforcement Network - GPEN*, la Rete Internazionale lanciata nel 2010, per promuovere una migliore cooperazione transfrontaliera in tema di *enforcement*, costituendo il Gruppo di coordinamento delle attività internazionali di *enforcement* (IECWG), volto a mettere in atto le raccomandazioni formulate durante l'evento internazionale di coordinamento *enforcement* svoltosi a Montreal nel 2012. Si sono tenute diverse *conference call* del IECWG durante le quali si è discusso, tra l'altro, del lavoro da svolgere per la redazione di un documento illustrativo di uno schema multilaterale di *enforcement* da adottarsi nel corso della 36ª Conferenza internazionale delle autorità di protezione dati. Tale documento dovrà fondarsi sullo schema di coordinamento delle attività internazionali di *enforcement* presentato alla 34ª Conferenza, nonché sull'attività del GPEN, e dovrà prendere in considerazione la condivisione delle informazioni connesse all'attività di *enforcement* nonché la gestione di tali informazioni da parte dei rispettivi destinatari. Il documento in corso di elaborazione non intende sostituirsi alle condizioni ed ai meccanismi già in essere a livello nazionale e regionale per quanto riguarda la condivisione di informazioni, né interferire con analoghi meccanismi operanti all'interno di altre reti. In ogni caso, è stata condivisa l'esigenza di elaborare un quadro multilaterale non legalmente vincolante.

Sempre al fine di migliorare le attività internazionali di *enforcement*, è stata decisa la messa a punto di una piattaforma informativa che offra uno "spazio sicuro" (GPEN *alert system*), dove le autorità responsabili dell'*enforcement* in materia di *privacy* possano condividere informazioni confidenziali e facilitare la promozione e conduzione di azioni coordinate di *enforcement*.

Infine, è proseguita anche l'attività del *PHAEDRA project*, progetto europeo (sostenuto anche dal Garante) volto a sostenere una migliore cooperazione e coordinamento tra i Commissari *privacy* e le autorità di protezione dei dati di tutto il mondo. Si tratta di un progetto biennale, promosso dal Consorzio costituito dalla Vrije Universiteit Brussel, Trilateral Research & Consulting, Università Jaume I di Madrid e l'Autorità polacca per la protezione dei dati personali. Il progetto mira – attraverso la cooperazione – a rendere più efficiente ed efficace l'uso delle risorse (sempre più limitate in questi ultimi anni) di cui dispongono le autorità di protezione dati e della *privacy* (v. par. 19.2).

Incontri con delegazioni estere e organizzazioni internazionali

L'Autorità ha proseguito la sua attività di partecipazione a programmi di partenariato europeo negli ambiti di competenza, in particolare nell'ambito dei programmi Taiex e Twinning e Icoiss della Commissione europea, offrendo la propria esperienza e competenza per facilitare l'avvicinamento delle normative dei paesi coinvolti al quadro comunitario in materia di protezione dei dati.

Nell'ambito di un quadro di collaborazione avviato con l'Autorità di protezione dati macedone risalente al 2008, anno in cui è stata firmata una dichiarazione di

mutua cooperazione, nel mese di aprile, il Garante ha ospitato delegati dell'Autorità macedone in visita-studio dedicata, in particolare, alla materia ispettiva. Inoltre, un delegato dell'Autorità ha partecipato al seminario sulla videosorveglianza nelle scuole, articolato in tre *workshop* che si sono svolti a Skopje nel mese di aprile.

Riguardo alla collaborazione con la Croazia, il Garante ha inviato propri esperti in occasione di alcuni *workshop* organizzati, nell'ambito del *Twinning* coordinato dall'Autorità spagnola di protezione dei dati, sui compiti e le responsabilità del *data protection officer* (7-8 e 27-28 febbraio) e di un seminario in materia di protezione dei dati personali e internet, tenutosi a giugno.

Nell'ambito del programma Icoiss finanziato dall'Unione europea, il Garante nel mese di settembre ha ricevuto una delegazione di alti dirigenti del Ministero dell'interno della Turchia, interessati al sistema della pubblica sicurezza a livello centrale e periferico.

Nell'ambito di un progetto di collaborazione accademica, inoltre, l'Università di Washington, con una delegazione composta da studenti e professori, ha avuto un incontro ufficiale con il Garante, in particolare sui temi del processo legislativo e sanzionatorio in Italia e negli USA e i profili di protezione dei dati legati a internet.

Il 10 settembre nella sede dell'Autorità, il relatore speciale delle Nazioni Unite per la promozione e la tutela della libertà di espressione, signor Frank La Rue è stato ricevuto dal Presidente del Garante. Nel corso dell'incontro, in vista del rapporto che l'inviato dell'Onu dovrà stilare e dell'incontro formale tenutosi il 13 novembre presso il Ministero degli esteri sui temi legati alla libertà di espressione nella rete con le diverse autorità competenti, sono state in particolare trattate le questioni del rapporto tra *privacy* e libertà di informazione, nonché le preoccupazioni per la proliferazione delle nuove forme di sorveglianza di massa, attraverso internet e i sistemi di telecomunicazioni, venute alla luce dopo il caso *Datagate*.

20 Comunicazione, divulgazione e trasparenza

20.1. *La comunicazione del Garante: profili generali*

La consapevolezza di vivere in una società che rischia di scivolare nella classificazione di massa e nella ipersorveglianza; il ricorso sempre più massiccio a sofisticate tecnologie di tracciamento, raccolta, conservazione e utilizzo delle informazioni – anche le più delicate – per le più svariate finalità, hanno indotto il Garante a mantenere alta nel 2013 l'attenzione ai problemi della sicurezza *online*, a livello nazionale ed internazionale e ad intensificare la sua azione di informazione e comunicazione a garanzia del rispetto del diritto alla protezione dei dati personali di ciascun individuo.

Con l'evoluzione della rete e delle tecnologie, che di giorno in giorno progrediscono e offrono al mondo possibilità che solo fino a qualche anno fa si ritenevano impossibili, per quanto il diritto alla protezione dei dati personali si sia affermato come uno dei pilastri della nuova cittadinanza, pare però sempre più spesso in pericolo. Nell'era digitale poter raccogliere, utilizzare, rielaborare dati è fondamentale e per il Garante è una sfida costante quella di fare in modo che lo sviluppo tecnologico si ponga in equilibrio con la protezione dei dati personali.

L'Autorità ha assicurato un'accurata informazione relativamente agli interventi operati riguardo a importanti settori del vivere sociale con i quali è di volta in volta chiamata a misurarsi: dalle intercettazioni ai problemi della sicurezza collettiva nazionale ed internazionale, dallo *spamming* (telematico e telefonico) al *marketing* comportamentale, da internet al *cybercrime* e alla violenza in rete, dal mondo dei *social network* al cyberbullismo, dalle tecnologie biometriche alle più svariate "tecnologie indossabili", capaci di tracciare ogni momento della nostra vita, dalle grandi banche dati alla lotta all'evasione fiscale, dalla trasparenza amministrativa alla sanità elettronica, dal giornalismo alla scuola. In questa cornice, il Servizio relazioni con i mezzi di informazione ha realizzato prodotti divulgativi allo scopo di offrire indicazioni operative per l'attuazione corretta delle norme, utilizzando le risorse *social* del web.

L'interesse dei *media* e, soprattutto, delle testate *online* per le tematiche riguardanti la protezione dei dati personali e l'attività del Garante è cresciuto rispetto allo scorso anno. Nel 2013 il Servizio relazioni con i mezzi di informazione ha selezionato oltre 43.000 articoli di interesse dell'Autorità. Sulla base della rassegna stampa prodotta giornalmente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali e dei *media online* che hanno trattato questioni legate generalmente alla *privacy* sono state quasi 13.000, delle quali 4.315 dedicate esclusivamente all'attività del Garante. Le prime pagine riguardanti i temi della protezione dei dati personali sono state oltre 770 (di cui 205 riguardanti la sola Autorità). Numerose sono state le interviste, gli interventi e le dichiarazioni pubblicate sulla carta stampata (636) e andate in onda su tv e radio nazionali e locali (63) nonché le citazioni relative all'attività del Garante in programmi televisivi e radiofonici nazionali (257).

20.2. *L'Autorità trasparente*

Particolare importanza ha rivestito l'impegno per l'attuazione delle misure normative in materia di trasparenza amministrativa cui l'Autorità ha dato attuazione con il Regolamento n. 1/2013 sugli obblighi di pubblicità e trasparenza relativi all'organizzazione e all'attività del Garante per la protezione dei dati personali (artt. 154 e 156, comma 3, del Codice) del 1° agosto 2013 (doc. web n. 2573442) e, quindi, disciplinato i periodi di tempo di pubblicazione di dati, informazioni e documenti del Garante con il provvedimento 17 ottobre 2013, n. 455 (doc. web n. 2753146). Nel sito istituzionale dell'Autorità, accessibile dalla *home page*, è stata creata la sezione "Autorità trasparente" che consente l'accesso immediato alle informazioni concernenti l'organizzazione e l'attività del Garante, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse assegnate, secondo criteri di facile accessibilità, completezza e semplicità di consultazione. Inoltre in collaborazione con tutti i dipartimenti e servizi del Garante è stato predisposto il Programma triennale per la trasparenza e l'integrità 2014/2016 dell'Autorità.

Alla voce "Procedimenti amministrativi" sono consultabili le procedure interne finalizzate alla tutela dei cittadini, in particolare quelle attinenti alla presentazione di reclami, segnalazioni e ricorsi nonché quelle relative all'attività di controllo e sanzionatoria ed agli altri procedimenti di competenza dell'Autorità. Molte altre sono le informazioni reperibili nella medesima pagina web: sui componenti del Collegio, l'organigramma e il personale, gli incarichi di collaborazione e consulenza, l'attività contrattuale ed il bilancio ed altre ancora.

20.3. *I prodotti informativi*

Nel 2013 sono stati diffusi 59 comunicati stampa e 15 *newsletter* (cfr. sez. IV, tab. 2).

La *newsletter* del Garante – che conta nella lista di distribuzione circa 3.600 destinatari – è una pubblicazione periodica che consente un ampio approfondimento sui principali provvedimenti adottati dall'Autorità nei diversi settori di intervento e sulle tematiche affrontate anche in ambito internazionale. Le notizie, redatte a cura del Servizio relazioni con i mezzi di informazione, per la versione web vengono composte graficamente e completate con l'aggiunta di immagini allo scopo di offrire un prodotto più sofisticato ed in linea con lo strumento web. La *newsletter*, giunta al suo XV anno di pubblicazione (per un totale di 382 numeri e di 1.323 notizie), viene inviata via *e-mail* a redazioni, professionisti, pp.aa., imprese e ai singoli cittadini che ne hanno fatto richiesta. Sul sito del Garante è inoltre attiva l'opzione "Iscriviti alla *newsletter*" (a disposizione di tutti i visitatori, allo scopo di garantire una quanto più ampia fruizione di questo importante strumento di informazione) ed è inoltre possibile consultare l'archivio tematico della *newsletter* che raccoglie, classificati per categorie, i 15 anni di articoli prodotti dal Servizio.

Infine, il numero dei comunicati stampa diffusi è raddoppiato rispetto allo scorso anno.

20.4. *I prodotti editoriali e multimediali*

Le campagne di comunicazione istituzionale del Garante, che nel 2013 si sono arricchite di nuovi prodotti, utilizzano diversi strumenti di divulgazione ed hanno la finalità di sensibilizzare il pubblico sulle tematiche riguardanti la protezione dei dati personali, e favorire la conoscenza dei mezzi di tutela e l'esercizio dei diritti.

Riguardo ai prodotti editoriali è stata predisposta una guida "Il condominio e la *privacy*" per facilitare un dialogo equilibrato tra tutti gli "abitanti" del condominio – dai condomini agli inquilini, dal portiere ai fornitori – che tiene conto dei casi di più frequente segnalazione nella vita condominiale, dall'assemblea all'accesso agli archivi, dalle comunicazioni agli interessati ai rapporti con l'amministratore, tenendo conto delle novità introdotte dalla riforma del condominio (entrata in vigore nel giugno 2013).

Sul fronte delle imprese, la mini guida "La *privacy* dalla parte dell'impresa" ha l'obiettivo di aiutare il settore privato a valorizzare e proteggere il proprio patrimonio di dati, trasformando la *privacy* da costo a risorsa senza ridurre la tutela dei diritti fondamentali della persona. L'opuscolo è stato anche tradotto in inglese per le tante imprese straniere presenti in Italia.

Per la parte multimediale sono state pubblicate due edizioni (la XXIV e la XXV) del Dvd "Il Garante per la protezione dei dati personali" – oggetto di distribuzione al largo pubblico in occasione di manifestazioni nazionali, convegni e seminari ai quali partecipa il Garante, oltre che essere inviato a quanti ne fanno specifica richiesta –, che raccoglie i principali provvedimenti adottati dall'Autorità, il glossario e una sezione "temi" con schede informative su argomenti di particolare interesse ed attualità. Come per tutte le precedenti edizioni, nell'archivio – sempre aggiornato – sono disponibili tutte le pubblicazioni dell'Autorità, in forma integrale e nell'originaria veste editoriale. Altre due aree tematiche, "normativa e informazione", consentono di accedere ai testi normativi, ai comunicati stampa ed alla raccolta completa della *newsletter*. In queste due sezioni i documenti sono stati reimpaginati per la consultazione video.

Sfruttando le opportunità offerte dal web e utilizzando linguaggi visivi più immediati ed accattivanti, pensati innanzitutto per un pubblico di "nativi digitali", sono stati realizzati alcuni video *tutorial*: "*Social network* connetti la testa" (http://www.gpdp.it/connettilatesta), per riflettere su come usare i *social network* in modo sicuro e consapevole, al quale è collegato anche un breve "questionario interattivo" (http://www.gpdp.it/connettilatesta/questionario) per testare il grado di consapevolezza dei pericoli presenti in rete, prodotti in occasione della Giornata europea della protezione dei dati personali; "Telefonate promozionali indesiderate. Come opporsi" (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1794339), per informare gli abbonati sulle norme che regolano il *marketing* telefonico e fornire le indicazioni utili per tutelarsi qualora non si vogliano più ricevere telefonate pubblicitarie; "Fatti *smart*" (http://www.gpdp.it/fattismart) con alcune utili indicazioni per tutelare la nostra *privacy* quando utilizziamo *smartphone* e *tablet*; "*Spam*, i consigli del Garante per difendersi" (www.garanteprivacy.it/spam), rivolto alla vasta platea degli utenti, contenente indicazioni utili per prevenire e contrastare la ricezione di messaggi commerciali indesiderati, se non addirittura molesti.

Tutti i video sono stati integralmente auto-prodotti, in tutte le fasi: scrittura e adattamento dei testi, sceneggiatura, sviluppo dell'animazione e selezione/costruzione degli elementi visivi, scelta delle musiche e sincronizzazione, registrazione dei testi audio, montaggio e post-produzione.

È stata inoltre sviluppata una strategia di promozione, anche attraverso tecniche di "viralizzazione" sui *social media* e di diffusione multicanale, messa a punto sulle esigenze di visibilità e sul profilo comunicativo specifico del Garante.

L'utilità e il gradimento dei prodotti sono stati riscontrati dall'elevato numero di visualizzazioni sui *social network* nei quali il Garante ha aperto appositi spazi (come You-tube e LinkedIn), nonché da vari articoli di apprezzamento apparsi sui giornali e su siti di esperti nel campo della comunicazione web.

Per ognuno dei prodotti video sono state create pagine tematiche dedicate, facilmente accessibili, ricche di informazioni e contenuti collegati, caratterizzate da una

grafica elaborata *ad hoc*. A fine anno è stata realizzata la scheda informativa "*Privacy* sotto l'albero" con utili consigli per la tutela della *privacy online* anche in vacanza (doc. web n. 2817431). Nelle statistiche del sito, le schede tematiche sono state tra le pagine più cliccate dagli utenti, raggiungendo anche diverse migliaia di visualizzazioni.

20.5. *Gli incontri internazionali*

Come illustrato al par. 19.2, l'Autorità italiana, rappresentata dal presidente, Antonello Soro, e dal segretario generale, Giuseppe Busia, ha partecipato alla 35ª Conferenza internazionale dei Garanti per la *privacy* tenutasi a Varsavia dal 23 al 26 settembre dal titolo "La *privacy*: bussola in un mondo turbolento" nonché alla Conferenza di primavera delle Autorità europee per la *privacy*, svoltasi a Lisbona dal 16 al 17 maggio, intitolata *Protecting privacy: the challenge ahead*, dedicata alle sfide che la protezione dei dati è chiamata ad affrontare con lo sviluppo delle nuove tecnologie.

20.6. *Le manifestazioni e le conferenze*

L'attività dell'Autorità collegata a convegni, seminari ed altre iniziative di carattere divulgativo ha riscontrato, anche nel 2013, un notevole interesse da parte del pubblico intervenuto.

Giornata europea della protezione dei dati personali

Il 28 gennaio è stata celebrata la Giornata europea della protezione dei dati personali. A partire dal 2007 questo è il giorno scelto per ricordare la data dell'adozione della Convenzione di Strasburgo n. 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato dei dati. Si tratta di un'iniziativa promossa dal Consiglio d'Europa con il sostegno della Commissione europea e di tutte le Autorità europee per la protezione dei dati personali, con l'obiettivo di informare i cittadini sui diritti legati alla tutela della vita privata e delle libertà fondamentali.

Il Garante ha voluto dedicare la Giornata al delicatissimo tema del cyberbullismo, chiamando a discuterne insieme il mondo della scuola e quello dei *social network*, al fine di sensibilizzare i giovani sui pericoli di un uso poco attento o responsabile delle nuove forme di comunicazione. In occasione della Giornata europea il presidente Soro ha inviato al Ministro dell'istruzione, dell'università e della ricerca una lettera (doc. web n. 2172284), auspicando che il tema del rispetto della riservatezza e della dignità delle persone nel mondo *online* venga assunto come momento imprescindibile di formazione per i giovani, allo scopo di aiutarli a conoscere realmente gli strumenti che abitualmente utilizzano ma di cui spesso ignorano i pericoli.

Il tema del cyberbullismo è stato trattato nell'ambito della trasmissione "Uno Mattina" della Rai Radiotelevisione italiana ed ha visto la partecipazione in studio del presidente dell'Autorità Antonello Soro insieme al Ministro dell'istruzione e ad un responsabile di Google Italia.

Trasparenza e p.a.

L'Autorità è stata presente anche nel 2013 al Forum PA – il più grande incontro europeo dedicato all'innovazione nella pubblica amministrazione – svoltosi a Roma dal 28 al 30 maggio. Tema guida della XXIV edizione è stato "Il Paese alla sfida della trasparenza e della verità"; sanità elettronica, trasparenza della p.a. e nuove regole *privacy* sono stati i temi principali affrontati dal Garante nel corso dei tre giorni della manifestazione. Martedì 28 maggio il primo seminario "*Privacy* e trasparenza della p.a.: un equilibrio necessario" è stato tenuto dalla vicepresidente, Augusta Iannini. Al centro del seminario la necessità di contemperare la piena trasparenza dell'attività svolta dalle pp.aa. con il diritto alla tutela della dignità e della riservatezza dei

cittadini, anche alla luce del d.lgs. n. 33/2013. In un secondo seminario, "*Privacy* e p.a.: l'organizzazione degli uffici e il *Data Protection Officer* alla luce del nuovo regolamento europeo" – sempre il 28 maggio – il segretario generale, Giuseppe Busia, ha trattato le principali novità contenute nella regolamentazione europea sulla *privacy* con particolare riguardo all'introduzione della figura del "responsabile della protezione dei dati". Il 29 maggio, nel corso del terzo seminario "Sanità elettronica e *privacy*", Licia Califano, componente dell'Autorità, ha affrontato le tematiche legate alla protezione dei dati in un settore particolarmente delicato, qual è quello della sanità, con particolare riferimento al Fse, all'*e-health*, alla telemedicina e al *cloud computing*.

Durante i tre giorni della manifestazione, presso lo *stand*, si è alternata la proiezione dei *video tutorial* divulgativi prodotti dal Garante e di un video appositamente realizzato contenente i tre filmati: "Proteggi il tuo mondo", "Pubblica intimità", "Una vita inscatolata", risultati vincitori del concorso "*Privacy* 2.0" organizzato in occasione dell'edizione 2012 della Giornata europea della protezione dei dati personali.

Nell'ambito della XXX Assemblea Anci (Firenze 23-25 ottobre) il Garante ha organizzato il seminario "La pubblica amministrazione tra domanda di trasparenza e protezione dei dati personali", dedicato al tema del corretto bilanciamento tra le finalità connesse alla pubblicazione delle notizie sull'attività amministrativa e il diritto alla riservatezza e alla dignità delle persone. Ai lavori, introdotti dal sindaco di Perugia, ha partecipato Licia Califano componente dell'Autorità che ha messo in guardia dai rischi per la vita privata derivanti da una diffusione indiscriminata e generalizzata di dati personali "basata su un malinteso e dilatato principio di trasparenza", ponendo l'accento sulla necessità che l'accessibilità alle informazioni del settore pubblico si coniughi con la tutela della *privacy* dei cittadini, a partire da quelli che ricevono sussidi economici pubblici perché versano in particolari condizioni di bisogno e disagio sociale.

Trasparenza amministrativa, digitalizzazione della p.a. e Agenda digitale sono altri temi sui quali è intervenuto il Presidente dell'Autorità partecipando a diversi incontri tra i quali:

"*Digital Government Summit* 2013: Attuare l'Agenda digitale: innovazione, sviluppo, democrazia" (Roma, 12-13 novembre). L'innovazione nel settore pubblico richiede la digitalizzazione della p.a., l'interoperabilità dei sistemi informativi, un'ampia e agevole disponibilità di dati e contenuti. Ne consegue un notevole incremento del numero e della tipologia di dati conservati all'interno dei diversi sistemi informativi. Il Presidente ha rappresentato l'importanza di prevedere, in primo luogo, rigorosi ed elevati *standard* per garantire la sicurezza e l'integrità delle diverse banche dati (compreso il profilo relativo alla interoperabilità delle stesse) e dei sistemi informativi, nonché la qualità dei dati in esse raccolti e dei soggetti legittimati ad accedervi. "Occorre privilegiare una politica di prevenzione" – ha sostenuto Soro – nell'ambito della quale l'Autorità può giocare un ruolo importante – con la consapevolezza che l'eventuale vulnerabilità delle infrastrutture è destinata ad arrecare gravi danni prima ancora che all'azione amministrativa ed alla qualità dei servizi offerti agli stessi cittadini. I dati archiviati e gestiti dalla p.a. appartengono infatti a singoli individui. Per questo non si può in nome dell'inevitabile progresso digitale abbandonare la logica dei diritti e non si può consentire, in nome della pura efficienza della p.a., un'indiscriminata raccolta di dati personali senza che venga posto alcun limite al loro possibile "sfruttamento", anche se per perseguire il "legittimo" fine di lottare contro gli sprechi e l'inefficienza.

All'incontro-dibattito "Trasparenza e *privacy* nell'amministrazione e nella giustizia amministrativa" – (Roma 13 aprile 2013) il Presidente, tracciata l'evoluzione del con-

certo di trasparenza amministrativa (dalla pubblicità all'accessibilità totale dei dati sancita dal decreto trasparenza), ha ricordato le indicazioni dell'Autorità, anche in sede di parere sul decreto, per garantire che la doverosa attività di "*disclosure*" e pubblicità dell'azione amministrativa non leda la dignità dei cittadini, rimarcando la tutela rafforzata di cui godono dati quali quelli sensibili e sanitari, in particolare, suscettibili di esporre l'interessato a discriminazioni, senza peraltro fornire alcuna informazione realmente utile all'esercizio del controllo diffuso sull'attività delle pp.aa.

Intervenuto al convegno "*E-Government* e *E-Justice* attraverso il *cloud computing*", organizzato a maggio presso il Dipartimento di scienze umane dell'Università europea di Roma, Soro ha rilevato che l'informatizzazione delle amministrazioni non è avvenuta in Italia con una visione d'insieme quanto, piuttosto, con processi frammentari e localistici che hanno determinato la creazione di sistemi autonomi, ciascuno dotato di proprie banche dati, contenenti spesso informazioni replicate e/o incongruenti in formati tra di loro incompatibili. L'utilizzo di servizi *cloud* da parte di una p.a. non può essere considerato in modo astratto e generico ma va attentamente studiato e calibrato sull'esigenza specifica del trattamento e sulla corretta identificazione dei dati da trattare, privilegiando atteggiamenti orientati alla prudenza come chiaramente suggerito, tra gli altri, dal WP29 nell'*Opinion* sul *cloud*, poiché "sviluppo tecnologico e protezione dati non sono in contrasto ma devono necessariamente trovare un giusto punto di equilibrio".

Datagate

Nel pieno svolgimento dello "scandalo mondiale di spionaggio", denominato *Datagate* (cfr. par. 19.3), l'Università degli Studi di Camerino ha organizzato una tavola rotonda dal titolo "La rete, i cittadini e i diritti" (Camerino, 12 novembre) nel corso della quale il presidente Antonello Soro è intervenuto sulla delicatissima questione del rapporto tra sicurezza e *privacy* nel contesto della rete globale, evidenziando il valore della tutela del diritto fondamentale alla protezione dei dati personali al tempo di *software* spia globali. "Oggi molti cittadini considerano la rete un rischio. Il *Datagate* – ha affermato Soro nel corso del suo discorso – ha rivelato che non c'è stata sintesi tra sicurezza e *privacy*, e che l'obiettivo della sicurezza ha prevalso sulla tutela dei diritti in generale e sul diritto fondamentale alla riservatezza. Il clamore dello scandalo con la grande presa di coscienza mondiale su questo tema che ne è derivata apre la strada ad un ripensamento che sposti il baricentro lungo l'asse sicurezza-*privacy* più nella direzione della difesa del diritto fondamentale al rispetto della persona umana e quindi della sua libertà e riservatezza". "Il *Datagate* – ha proseguito – ha favorito una presa di coscienza sui cambiamenti dell'idea di libertà che ha sempre più a che fare con la responsabilità dell'immagine che diamo di noi stessi – e ha aggiunto – come nella sfera digitale la nostra immagine dipende molto anche dagli altri, perché il controllo su di essa è assente". "Vicende come il *Datagate* – ha concluso Soro – rendono chiaro a tutti che i dati personali rappresentano un valore da proteggere, un bene prezioso da difendere". Sullo stesso tema il Presidente è intervenuto anche alla giornata di studio del 6 dicembre presso la Camera dei deputati dedicata a "*Datagate* e *privacy*. Dati segreti, dati spiati, dati venduti". Qui, Soro ha ricordato i tre fattori che hanno prodotto il *Datagate*: le leggi emergenziali approvate dopo l'11 settembre 2001; la vulnerabilità dei cavi di fibre ottiche su cui viaggiano le trasmissioni transoceaniche; la concentrazione di enormi quantità di informazioni personali nei *server* dei "*big* della rete", come Google e *Facebook*. Tutto ciò ha determinato una gravissima perdita di fiducia dei cittadini nei confronti del Governo Usa e negli stessi colossi di internet. "Con il *Datagate* – ha sottolineato Soro – ci siamo trovati in presenza di un 'effetto paradosso': quello di un governo democratico che per combattere il terrorismo e difendere la libertà delle persone viola massicciamente questa stessa libertà, che non è solo quella dei cittadini americani, ma anche di quelli europei e di altri paesi del

mondo". Il *Datagate* ha dimostrato, secondo Soro "quanto possa essere rischiosa – per la democrazia e i diritti di tutti i cittadini del mondo – la combinazione tra la concentrazione in un unico Paese dei principali *provider* e leggi emergenziali che considerino le libertà un lusso cui, necessariamente, rinunciare. Rischi, questi, ulteriormente aggravati dalla vulnerabilità dei sistemi informatici e ancora di più dei cavi di fibra ottica cui sono affidati, assieme alle comunicazioni, interi pezzi della vita privata di ciascuno di noi e che norme emergenziali hanno reso facilmente accessibili, almeno negli snodi americani, alle agenzie di *intelligence*". "L'Unione europea – ha ricordato Soro – ha tentato di fare luce sulla vicenda, istituendo un gruppo di lavoro con funzione conoscitiva, il cui limite maggiore risiede, però, nel segreto opposto dagli Usa su alcune informazioni che sarebbe stato invece necessario acquisire per meglio comprendere caratteristiche e dimensioni del fenomeno".

Per quanto riguarda, in particolare, il nostro Paese, Soro ha sottolineato come il protocollo siglato tra Garante e il Dis, (Dipartimento informazioni per la sicurezza), rappresenti "una risposta positiva" alle preoccupazioni suscitate dal *Datagate*, una risposta in grado, peraltro, di portare a sistema l'attività di vigilanza del Garante e consentire una ricognizione degli archivi utilizzati dai Servizi. Soro ha concluso il suo intervento sottolineando come sempre di più "*privacy* è un altro nome della libertà".

Internet

Al convegno "La libertà di informazione che vorremmo, quella che abbiamo e quella che rischiamo di non avere" (14 novembre) i cui lavori sono stati introdotti dal Presidente del Senato e la Presidente della Camera, il presidente Soro è intervenuto nella seconda sessione dedicata al tema del "Diritto all'oblio o oblio dei diritti?". "La rete non può essere luogo dell'oblio dei diritti – ha sostenuto il Presidente del Garante – nello spazio digitale la rappresentazione che si ha di sé dipende solo in parte dall'individuo, per il resto è determinata da altri. Obiettivo del Garante è ricongiungere l'identità digitale con quella reale cercando un punto di equilibrio, da un lato sottraendo informazioni ai motori di ricerca, dall'altro facendo aggiornare le informazioni con dati rilevanti successivi".

A marzo, presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Firenze, si è tenuto il convegno "Nuovi mezzi di comunicazione e identità: omologazione o diversità?" nel corso del quale il presidente Soro ha analizzato gli effetti che la diffusione dei *social media* e, in genere, delle nuove tecnologie hanno sulla riservatezza individuale, evidenziandone opportunità ma anche rischi, soprattutto a fronte del crescente dilagare dell'*hate speech*. Il presidente Soro ha illustrato alcune possibili soluzioni incentrate su un equo bilanciamento tra garanzia della libertà della rete e tutela della riservatezza individuale, per evitare che la rete, da strumento di libertà e democrazia, divenga spazio anonimo in cui impunemente violare i diritti e la dignità altrui.

Il Garante, da sempre impegnato sul fronte della tutela dei minori, ha svolto negli ultimi anni una decisa azione a protezione dei giovani sulla rete, cercando di sensibilizzare l'opinione pubblica, le famiglie e la scuola. Il tema della "Violenza mediatica sui minori" è stato affrontato da Licia Califano, componente dell'Autorità, al convegno svoltosi a Pesaro il 20 aprile. "I *social network* – ha detto la Califano nel suo intervento – rappresentano uno strumento straordinario a disposizione dei giovani per dialogare, scambiarsi opinioni, cercare informazioni, esprimere idee ed emozioni, essere in contatto con il mondo. Ma quando i *social network*, come avviene per il fenomeno del cyberbullismo, vengono usati per umiliare, offendere, denigrare i coetanei, queste potentissime forme di comunicazione e condivisione si trasformano in strumenti di abuso e violenza, mostrando in maniera drammatica un 'lato oscuro' della rete che dobbiamo imparare a conoscere, prevenire e combattere".

Sanità

A giugno, il presidente Soro è intervenuto al convegno "Sanità sul *cloud*: Istruzioni per l'uso" (Roma, 24 giugno). L'assistenza sanitaria, nell'era digitale, può avvantag-

giarsi delle più svariate opportunità e potenzialità offerte dall'uso delle tecnologie. Tuttavia, maggiori sono i servizi offerti *online*, maggiori sono i dati sensibili trattati cui il Codice accorda particolare cautela in ragione della loro idoneità ad incidere su diritti e libertà fondamentali dell'interessato. Se dunque la creazione di sistemi nazionali di sanità elettronica, è un obiettivo di rilevante interesse pubblico, deve però essere raggiunto – secondo il Presidente dell'Autorità – in un quadro giuridico di garanzie che i legislatori nazionali sono chiamati a rendere operative. Le diverse modalità di utilizzo delle tecnologie, con differenti modelli organizzativi, frutto anche di una differenziata capacità di investimento, potrebbero essere superate adottando modelli uniformi di *cloud*, con la pur necessaria prudenza nella scelta di tali tecnologie.

Licia Califano ha altresì partecipato al *meeting* nazionale "Il Fascicolo sanitario elettronico in Italia" tenutosi a Napoli dal 13 al 15 giugno nel quale si sono incontrati i massimi esperti di *e-health* per discutere dello stato di attuazione del Fse in Italia e delle prospettive future.

Il Garante nel cambiamento

Al *Consumers' Forum* - "*Authority* e consumatori. La regolamentazione ai tempi della crisi" (Roma, 26 novembre), il presidente Soro ha auspicato un incremento della collaborazione tra Autorità garanti e ha sottolineato come sia indispensabile la ricerca di un punto di equilibrio tra la tutela dei dati personali – definiti un patrimonio prezioso da proteggere – e una efficace lotta all'evasione, riferendosi in particolare, all'intervento dell'Autorità in materia di reddirometro.

Augusta Iannini è intervenuta alla 3ª edizione del "*Privacy day forum*" (Roma, 23 maggio 2013), l'annuale appuntamento organizzato da Federprivacy per quanti si occupano di protezione dati e per chi vuole tenersi aggiornato sul tema illustrando "come si è evoluta l'Autorità per raccogliere le sfide della *privacy*" nella prospettiva della proposta di regolamento europeo, volto ad assicurare uniformità normativa in tutti gli Stati membri.

20.7. *Le relazioni con il pubblico*

Nello svolgimento dei propri compiti istituzionali l'Autorità esprime, attraverso l'Ufficio relazioni con il pubblico, la più compiuta forma di vicinanza alla collettività, riscontrandone le istanze attraverso un servizio ispirato ai principi di efficacia e trasparenza, anche in conformità al Regolamento sugli obblighi di pubblicità e trasparenza relativi all'organizzazione e all'attività del Garante (artt. 154 e 156, comma 3, del Codice) del 1° agosto 2013, n. 380 (in G.U. 19 giugno 2013, n. 193, doc. web n. 2573442).

L'Ufficio relazioni con il pubblico è strutturato come luogo di incontro, privo di formalità, tra l'Autorità e gli interessati, improntato alla massima accoglienza e cortesia, ove i quesiti e le istanze di ciascuno sono oggetto di attenta disamina anche al fine di diffondere la conoscenza della disciplina della protezione dei dati personali.

Le numerosissime istanze rivolte all'Urp vengono ricevute, esaminate e riscontrate con sollecitudine, non di rado anche nel giro di poche ore, con le modalità ritenute più idonee alla tipologia di richiesta.

Non è da trascurare inoltre il ruolo aggregante che l'Urp svolge nei confronti di tutte le unità e dipartimenti dell'Autorità, consentendo così di migliorare l'organizzazione interna dell'Ufficio a vantaggio della tutela dei diritti delle persone.

L'attività dell'Urp

L'attività dell'Urp si sostanzia preliminarmente nel ricevere quesiti o richieste di pareri ai quali l'Ufficio fornisce riscontro in tempi celeri e, ove possibile, anche in tempo reale, utilizzando strumenti duttili e veloci come la posta elettronica o il colloquio telefonico, rendendo così possibile una tempestiva trattazione delle problematiche.

Le aree di intervento su cui l'attività dell'Urp incide sono così sintetizzabili:

- indirizzo: l'Ufficio, ricevuta l'istanza, la esamina prontamente in punto di diritto, valutando se al quesito può essere dato riscontro, indirizzando il richiedente verso provvedimenti già adottati dall'Autorità oppure informandolo sul tema d'interesse, ricorrendo, nel caso, anche all'ausilio di note predisposte dall'Ufficio, offrendo in tal modo un servizio di supporto alla scelta dello strumento di tutela più idoneo previsto dal Codice;
- interscambio con l'utenza: l'Urp, per definizione luogo deputato ad accogliere le molteplici istanze del pubblico, diviene anche "osservatorio privilegiato" delle tematiche di maggior interesse, consentendo dunque di intercettare le questioni che più incidono sulla vita delle persone, trasferendo tali sollecitazioni direttamente all'Autorità. Si può certamente affermare in questo senso che il predetto ufficio svolge un'azione di ponte tra la collettività e l'Autorità;
- informativa: la diffusione della conoscenza della normativa in materia di protezione dei dati personali ha modo di realizzarsi compiutamente proprio nel rapporto diretto con le persone che, recandosi fisicamente presso l'Ufficio, oppure utilizzando il telefono, o la posta elettronica, si rivolgono all'Urp con quesiti e, più in generale, formulando richieste di chiarimenti sulla normativa. L'Ufficio fornisce un *feed back* in tempi strettissimi e, quando possibile, nel corso della stessa giornata, restituendo all'esterno una solida reputazione di affidabilità ed efficienza del servizio reso. Le modalità di risposta dell'Ufficio, pur ormai consolidate, sono comunque sempre oggetto di attenta valutazione per potenziali miglioramenti del servizio, anche in considerazione delle nuove possibilità di interazione con l'esterno. Per effetto della continua ricerca volta al perfezionamento di queste articolate modalità di relazione con il pubblico, anche nell'arco del trascorso anno di attività, l'Ufficio ha raccolto numerosissime attestazioni di gradimento per il servizio erogato, confermando il *trend* positivo ormai consolidato che viene riscontrato presso l'utenza (rapporto "qualità erogata" e "qualità percepita").

Anche per questo anno di attività, tra i settori più frequentemente portati all'attenzione dell'Autorità (cfr. per una panoramica completa il grafico 17 nella sez. IV della Relazione) non si può non menzionare ancora il tema del *direct marketing* soprattutto telefonico, fenomeno del quale il cittadino lamenta la particolare aggressività sia per la frequenza del disturbo durante l'arco della giornata, sia per le modalità colloquiali utilizzate dagli operatori. La denunciata insopportabile insistenza e, talora, la maleducazione degli operatori di *call center*, gli orari di chiamata spesso inopportuni, le scorrettezze commerciali, quali l'attivazione di servizi non richiesti, rappresentano ancora un'importante area della quale si chiede a gran voce una soluzione definitiva, anche attraverso il Garante. Da non trascurare l'attività di *marketing* svolta attraverso strumenti informatici o l'invio meccanizzato di fax promozionali con conseguente violazione, spesso in orari notturni, della sfera di riservatezza delle utenze telefoniche private o, nel caso di contatto di utenze presso uffici, negozi o studi medici, di intralcio all'attività lavorativa.

Un'attenzione molto alta si è potuta registrare relativamente alle richieste di informazioni circa gli adempimenti previsti dal Codice (complessivamente il 12% delle *e-mail* trattate) necessari per far valere le prerogative sottese al diritto alla protezione dei dati personali. Molto apprezzato è l'ausilio nell'esercizio delle forme di tutela che prevedono una maggiore formalità come ad esempio la proposizione del ricorso.

Va segnalato inoltre che, a seguito dell'entrata in vigore, nel giugno 2013, della legge di riforma della disciplina del condominio negli edifici (l. n. 220/2012), sono significativamente aumentate le richieste di chiarimenti in tale settore soprattutto

per quanto attiene alla costituzione del cd. registro dell'anagrafe condominiale. Anche il recentissimo d.lgs. n. 33/2013 (cd. decreto trasparenza) ha proposto nuovi temi di indagine circa l'impatto di tale normativa sulla disciplina relativa alla protezione dei dati personali.

La valutazione complessiva dei dati statistici riguardanti l'attività dell'Urp conferma un *trend* costante di attenzione dell'utenza per la tutela del diritto alla protezione dei dati personali. Nell'ambito dell'attività di *front office*, infatti, i contatti registrati nel periodo di riferimento sono complessivamente pari a 31.134 (contatti telefonici, *e-mail*, visitatori, fascicoli), di cui 12.800 a mezzo telefono e 17.654 mediante *e-mail* o posta ordinaria (cfr. tabelle 2 e 16). A questi dati vanno aggiunti 304 fascicoli trattati nel corso del 2013 (cfr. sez., IV, tab. 16).

Particolare gradimento si è registrato rispetto all'attività di ricevimento dei visitatori, circa 376 unità (cfr. sez. IV, tab. 16). In questi casi è importante ricordare, oltre l'attività di assistenza, anche l'attività divulgativa che l'Ufficio svolge, distribuendo all'occorrenza, oppure ove richiesto, il materiale informativo messo a disposizione dall'Autorità. Per l'anno in corso risultano essere state particolarmente apprezzate, per chiarezza e fruibilità, le pubblicazioni in materia di "Condominio e *Privacy*" e "La *privacy* dalla parte delle imprese".

Un attento *screening* dei dati elaborati dall'Ufficio ci informa inoltre dei diversi *target* di utenza talché è possibile anche modulare le tipologie di riscontro a seconda che il richiedente sia un soggetto pubblico, un operatore di un settore specifico, dotato di una già approfondita conoscenza della materia, piuttosto che un privato cittadino più o meno informato.

Tematiche d'interesse

Il tema del *marketing* telefonico è stato quello con il maggior numero di segnalazioni (3.834) confermando purtroppo, ormai a tre anni dall'entrata in vigore della disciplina relativa al Registro pubblico delle opposizioni, un *trend* negativo rispetto alla effettività di tutela fornita. Se da un lato il cittadino non si è avvantaggiato dei benefici sperati con l'adozione del Registro pubblico delle opposizioni, dall'altro si può evidenziare certamente una maggiore informazione e consapevolezza dei diritti in questione, comprovati anche da segnalazioni strutturate, complete degli elementi necessari per consentire all'Autorità una compiuta istruttoria.

Rispetto all'anno precedente, la percentuale di richieste di intervento in materia di attività di *marketing* svolte attraverso altri canali, quali la posta cartacea, le *e-mail* e i fax pubblicitari indesiderati, è rimasta pressoché invariata (2.321). In relazione a questo tema, l'Ufficio ha svolto un'attività analoga a quella sopra descritta concernente segnalazioni di ricezione di *e-mail* e fax indesiderati e per altre questioni legate al *marketing*.

In altri settori si è registrato un consolidamento e, in alcuni casi, anche un incremento del numero di segnalazioni/richieste di informazioni. Rappresentano ciascuna una quota tra il 4% e il 5% del totale le questioni relative alla videosorveglianza e al trattamento dei dati personali nella gestione del rapporto di lavoro, mentre in ambito giornalistico (anche *online*) la quota è pari al 2%; si registra, infine, a seguito dell'adozione del d.lgs. n. 33/2013, un incremento nei quesiti relativi al tema della trasparenza amministrativa.

Resta sempre alto il numero di richieste di informazioni e di segnalazioni in materia di videosorveglianza (820 *e-mail*), concernenti soprattutto il settore del lavoro nonché gli adempimenti previsti dal provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680), con particolare riferimento ai casi in cui è necessario ricorrere ad una richiesta di verifica preliminare (art. 17 del Codice) e ai tempi di conservazione delle immagini. Si registra un incremento dell'attenzione rispetto all'utilizzo della videosorveglianza in ambito condominiale oltre che personale e domestico, come pure per i dispositivi funzionanti a bordo di veicoli privati (*dashcam*).

Risulta altresì significativo il numero delle segnalazioni e dei quesiti relativi a trattamenti di dati personali nell'ambito dei rapporti di lavoro (787 *e-mail*), sia pubblico che privato. Le tematiche maggiormente ricorrenti si confermano essere quelle relative ai trattamenti di dati biometrici, così come quelle relative all'utilizzo di internet e posta elettronica in ambito aziendale, il controllo a distanza dei lavoratori ed il trattamento di dati sensibili correlati al riconoscimento di permessi o benefici, mentre il tema della geolocalizzazione si arricchisce di nuove modalità operative, dispositivi elettronici molto diffusi ed assai subdoli nel carpire informazioni e nell'effettuare i controlli dei dipendenti (v. uso di *tablet* o *smartphone* a fini rilevazione delle presenze dei lavoratori).

Si registra una flessione rispetto al settore del credito le cui istanze riguardano per lo più l'oggetto e le modalità dell'esercizio del diritto di accesso ai propri dati bancari. Altri profili riguardano la pertinenza e non eccedenza delle informazioni richieste dalle banche circa l'applicazione della normativa in materia di antiriciclaggio (d.lgs. 21 novembre 2007, n. 231) e le comunicazioni a terzi di informazioni bancarie.

Per quanto riguarda l'attività di recupero del credito (404 *e-mail*), si registra una persistente aggressività nelle modalità di contatto dei debitori (visite al domicilio o sul luogo di lavoro, sollecitazioni telefoniche non solo presso i recapiti del debitore, ma anche presso familiari, vicini di casa, datori di lavoro) con una conseguente lesione della riservatezza e della dignità delle persone coinvolte. Inoltre, sempre nel settore del credito, risultano ancora frequenti le richieste di assistenza finalizzate ad attivare le procedure di aggiornamento, correzione, cancellazione di dati personali trattati dai sistemi informativi privati in materia di credito al consumo e puntualità e affidabilità nei pagamenti (286 *e-mail*).

Altro settore in cui è possibile registrare un netto incremento in termini di richieste di informazioni da parte del pubblico è sicuramente quello legato ai *social network*. La sempre maggiore diffusione unitamente alla gravità dei fatti di cronaca legati all'uso di tali strumenti (episodi di cyberbullismo) implica una serie di criticità anche sul versante della applicabilità della normativa italiana rispetto a trattamenti che spesso vengono effettuati da titolari aventi sede all'estero.

Altro tema legato alla *privacy* in rete di cui si registra un notevole incremento è quello legato alla disciplina relativa all'uso dei cd. *cookie* e di altri strumenti analoghi (*web beacon/web bug, clear* GIF, *etc.*) installati nei terminali degli utenti (personal computer, *notebook*, *tablet pc*, *smartphone*, *etc.*), soprattutto per le novità introdotte a seguito dell'attuazione della direttiva 2009/136 che ha modificato la direttiva "*e-Privacy*" (2002/58/CE).

Si registra un aumento del numero di quesiti in materia di trasferimento all'estero di dati personali soprattutto in riferimento alle corrette modalità da seguire da parte dei soggetti coinvolti nell'ambito della cd. procedura BCR (art. 44, comma 1, lett. *a*), del Codice).

Pressoché invariate nel numero risultano essere le richieste di informazioni in materia di *privacy* e giornalismo, soprattutto in relazione alla corretta gestione dei cd. archivi storici *online* dei quotidiani. Infatti l'indicizzazione di articoli giornalistici che permangono accessibili attraverso i comuni motori di ricerca nonostante sia trascorso un ragionevole lasso di tempo rispetto all'accadimento dei fatti resta un fenomeno piuttosto diffuso nonostante le pronunce dell'Autorità sul tema del diritto all'oblio.

Per quanto riguarda il settore pubblico, il d.lgs. n. 33/2013 sulla trasparenza così come la l. n. 190/2012 sull'anticorruzione hanno introdotto una serie di adempimenti per gli enti pubblici forieri di numerose questioni interpretative (concernenti, in particolare, l'obbligo di pubblicazione dei redditi e dei dati patrimoniali di consiglieri, assessori e sindaci, la pubblicazione sui siti degli istituti scolastici dei decreti di forma-

zione delle classi così come la pubblicazione dei compensi accessori degli insegnanti derivanti dall'utilizzo dei fondi di istituto) sulle quali l'Autorità ha intrapreso un'attività di approfondimento. Su questi temi infatti le indicazioni contenute nelle linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web del 2 marzo 2011 (doc. web n. 1793203) (e già nelle linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali del 19 aprile 2007, doc. web n. 1407101) necessitano di essere rimodulate in relazione alla nuova disciplina introdotta dalle fonti menzionate.

Ancora ricorrenti risultano essere le richieste di parere in materia di accesso ai documenti amministrativi sia da parte dei cittadini, sia da parte dei consiglieri comunali, agli atti degli enti locali per i quali, come noto, l'Autorità non ha tuttavia competenza ad esprimersi in ordine al rilascio o meno degli atti richiesti.

20.8. *Il Servizio studi e documentazione*

La redazione della Relazione annuale

Il Servizio studi ha coordinato la preparazione del testo della Relazione annuale per la presentazione al Parlamento.

Si tratta di un importante adempimento istituzionale dell'Autorità, espressione dei caratteri dell'indipendenza e dell'autonomia, divenuto nel tempo un'importante occasione di riflessione e analisi anche interna sull'attività svolta, soprattutto ai fini della programmazione e dei possibili miglioramenti nello svolgimento delle funzioni del Garante, tra le quali quella di curare, anche attraverso il sito istituzionale, la conoscenza da parte del pubblico della disciplina in materia di protezione dati.

La funzione di studio e di supporto giuridico

Il Servizio ha effettuato studi ed approfondimenti su questioni tecnico-giuridiche di interesse dell'Autorità, ed ha raccolto e trasmesso alle strutture richiedenti documentazione e sintetiche osservazioni su questioni di interesse.

Tra l'altro sono stati svolti approfondimenti sullo schema del regolamento di un'autorità indipendente in materia di tutela del diritto d'autore; sulla proponibilità del ricorso al Garante da parte del curatore dell'inabilitato e l'esercizio dei diritti di cui all'art. 7, del Codice; sul concetto di "finalità" e "trattamento compatibile" in relazione ad una bozza di parere del WP29; sul concetto di "profilazione" come trattamento distinto da quello di *marketing*; inoltre, su iniziativa del Servizio, in ragione dell'importanza del provvedimento, sono state formulate osservazioni sullo schema di d.lgs. attuativo dell'art. 1, comma 35, l. n. 190/2012 in materia di obblighi di pubblicità, trasparenza e diffusione delle informazioni da parte delle pp.aa.

È stato altresì effettuato un approfondimento, su richiesta del Collegio, sui poteri del Garante in relazione ai trattamenti di dati effettuati nell'esercizio della libertà di espressione, con particolare riferimento all'*e-book*, ed è stato esaminato il testo preliminare, elaborato dal competente gruppo di lavoro, delle linee guida in materia di biometria. Alcune considerazioni – essenzialmente di metodo – sono state espresse su ipotesi di riorganizzazione dell'Ufficio.

I pareri sulle leggi regionali

Il Servizio ha costantemente 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, ai sensi dell'art. 127 Cost., delle leggi regionali non conformi ai principi e alla disciplina sulla protezione dei dati personali (*supra* par. 3.3).

Come negli anni precedenti, i testi legislativi esaminati sono risultati, di massima, rispettosi dei limiti di cui all'art. 117 Cost., anche alla luce di quanto deciso dalla Corte costituzionale (sent. n. 271/2005) sulla competenza legislativa esclusiva dello

Stato in materia di protezione dei dati personali, nonché dei principi e delle disposizioni contenuti nella normativa internazionale (art. 8 Cedu) e comunitaria.

In particolare, profili di illegittimità sono stati prospettati con riferimento ad una norma di una legge sul procedimento amministrativo che ha riconosciuto a tutti, senza obbligo di motivazione, il diritto di accesso, in termini che sono apparsi non consentire la verifica, tra l'altro, dell'attualità dell'interesse, anche con riferimento all'indispensabilità dell'accesso ai sensi dell'art. 24 u. c. l. n. 241/1990 per i dati idonei a rivelare stato di salute e vita sessuale.

Il Servizio, analogamente agli anni passati, ha curato l'aggiornamento del personale attraverso la redazione di due notiziari interni:

I servizi interni di documentazione

- il "Repertorio di documentazione su diritti, libertà fondamentali e dignità della persona" denominato "Osservatorio *privacy*", una rassegna periodica di normativa, dottrina e giurisprudenza nazionale, comunitaria ed internazionale su questioni di interesse per l'Autorità, suddivisa in un'ampia sezione di principi generali e in sezioni più specialistiche, corrispondenti alle macro-aree tematiche di attività del Garante: libertà pubbliche e sanità; comunicazione e reti telematiche; realtà economiche e produttive; lavoro; amministrazione, contratti e risorse umane. Si sono anche proposti alcuni spunti di approfondimento sul valore economico dei dati personali;
- il "Servizio studi *news*", strumento di monitoraggio della giurisprudenza, anche comunitaria ed internazionale in materia di diritti e libertà delle persone e protezione dei dati personali, con il quale si è cercato di seguire da vicino la giurisprudenza della Corte EDU che, per la ponderazione tra diritti contrapposti, costituisce riferimento per la Cgue e le varie giurisdizioni nazionali (v. ad es., sul margine di apprezzamento spettante agli Stati aderenti per quanto riguarda il bilanciamento tra libertà di espressione e protezione della vita privata, la decisione Corte EDU del 16 luglio 2013, su ricorso n. 33846/07, relativa alla permanenza, nel sito internet di un giornale, di un articolo giornalistico ritenuto in precedenti giudizi interni basato su informazione insufficiente e lesivo dei diritti della persona interessata). In questa prospettiva si è riservato un certo spazio anche alle decisioni di giudici di *common law* e segnatamente britannici, per cercare di illustrare il modo in cui esse dànno conto delle peculiarità dei singoli casi nell'applicazione di principi (per diversi aspetti) comuni.

Il Servizio ha altresì contribuito all'organizzazione di seminari interni su tematiche giuridiche e tecnico-informatiche per la formazione e l'aggiornamento del personale, curandone in particolare uno sulla disapplicazione d'ufficio del diritto interno contrastante con quello comunitario, di particolare rilievo per l'Autorità al fine di assicurare, in posizione di indipendenza, una effettiva tutela degli interessati nei confronti di soggetti pubblici e privati.

20.9. *La Biblioteca*

La Biblioteca nasce nel 2001 e rappresenta un'articolazione della Segreteria generale. Il suo compito istituzionale consiste nel raccogliere, organizzare, inventariare, classificare con criteri bibliografici, conservare e valorizzare le pubblicazioni italiane e straniere attinenti alla disciplina della protezione dei dati. In raccordo con il dettato normativo, l'incremento del patrimonio della Biblioteca si estende alle tematiche dei diritti e delle libertà fondamentali, della dignità, della riservatezza e della identità personale.

Il patrimonio della Biblioteca ha raggiunto 14.676 volumi monografici (circa 7.500 in lingua straniera) e 400 testate di periodici, delle quale 36 correnti (dati

aggiornati al 31 dicembre 2013). La Biblioteca dispone di un Fondo speciale, costituito da una donazione del prof. Rodotà, che annovera più di 1.500 volumi e materiali bibliografici 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. Presso la Biblioteca esiste inoltre un deposito di circa 200 tesi italiane di laurea e di dottorato in materia di protezione dei dati.

Dal 2004 sulla rete intranet è consultabile il catalogo OPAC dei titoli posseduti, con 5.372 volumi inseriti (5.054 monografie); gli aggiornamenti del catalogo informatizzato delle acquisizioni successive al 2004 vengono pubblicati sul sito web della Biblioteca.

La Biblioteca è nata per svolgere essenzialmente una funzione amministrativa e per agire da supporto alle attività di informazione, di ricerca e di studio dell'Autorità. Ma la diffusione dell'interesse nel campo della *privacy* e della *data protection* rende ormai necessario un ripensamento di questa finalità originaria ed un'apertura al mondo dello studio e della ricerca in ambito istituzionale e, in particolare, accademico. Dopo il riordino delle collezioni completato nel 2012 si è pertanto proceduto ad una nuova catalogazione analitica del posseduto attraverso la creazione di un *thesaurus* di termini-chiave collegato alle acquisizioni di materiali bibliografici italiani e internazionali dell'ultimo biennio (2012-2013). In tal modo, la Biblioteca ha iniziato a sperimentare un modello di indicizzazione sistematico che utilizza le potenzialità dei *Linked Open Data*. L'obiettivo perseguito è quello di ultimare entro il 2014 il *thesaurus* delle sezioni tematiche con la raccolta di monografie e di documenti strettamente dedicati alla protezione dei dati (circa 4.800 volumi). Queste sezioni comprendono nell'ordine: a) la raccolta completa delle pubblicazioni a stampa dell'Autorità; b) la letteratura italiana sulla riservatezza e sulla protezione dei dati, con particolare riguardo alle pubblicazioni successive alla costituzione dell'Autorità; c) la letteratura italiana sulle autorità indipendenti; d) le pubblicazioni a stampa delle autorità sulla protezione dei dati dei Paesi membri della UE; e), f), g) e h), la letteratura mondiale sulla *data protection*, suddivisa nelle macro-aree culturali tedesca, francese, spagnola e anglo-americana.

La Biblioteca costituisce una singolarità a livello nazionale ed europeo sotto numerosi punti di vista. Il Garante risulta difatti unica autorità di controllo nella UE ad avere istituito una biblioteca imperniata specificamente sulla protezione dei dati. E la stessa dimensione numerica delle collezioni, estese sul duplice piano della bibliografia contemporanea e di quella storica, rappresenta un fattore di grande rilievo nel panorama delle istituzioni bibliotecarie italiane e internazionali. Alla luce dei più aggiornati riscontri statistici comparati, il sistema SBN cataloga circa 2000 titoli (dei quali circa 800 in lingua italiana) sulla tematica della riservatezza, del *right to privacy* e della *data protection*. Il Polo Bibliotecario Parlamentare totalizza circa 1000 titoli (dei quali circa 700 italiani). In Germania, la *Deutsche Nationalbibliothek* conta 1384 titoli con ricerca sul vocabolo *privacy* (635 monografie) e 3.771 titoli con ricerca sul vocabolo *Datenschutz* (2696 volumi). Negli Stati Uniti, la principale biblioteca giuridica mondiale, la *Harvard Law School Library*, possiede 6670 volumi sul vocabolo *privacy* (6.327 monografie, delle quali 632 pubblicate nell'ultimo triennio e 2.659 negli ultimi dieci anni) e 3.399 volumi sulla combinazione di *privacy* e di *data protection*.

La moltiplicazione dei campi di intervento dell'Autorità impone, d'altro canto, l'aumento delle risorse disponibili soprattutto sul piano del costante aggiornamento e della completezza e rapidità dell'informazione. Il progetto di *Digital Library*, avviato nel 2008 in cooperazione con il Dipartimento risorse tecnologiche, è stato pertanto arricchito dalle nuove *e-book libraries* consultabili sulla rete intranet.

Accanto alle "strategie di possesso" (imperniate sull'incremento del patrimonio cartaceo) sono state potenziate le "strategie di accesso" concentrate negli archivi *full-text* pubblicati in formato elettronico. L'attuazione di un piano di acquisizione triennale di *database* ha concretizzato tale impostazione. Il sito web della Biblioteca, trasformato in portale, è stato riorganizzato sulla base della suddivisione in aree funzionali, in modo da coordinare tutte le risorse bibliografiche elettroniche (l'OPAC *online* e i *database*) nel quadro di una complessa *knowledge infrastructure* e *knowledge organization*: questa architettura di conoscenze condivise ha lo scopo di fornire una serie di strumenti qualificati per le attività del Collegio e per il lavoro dei dipartimenti e dei servizi nei rispettivi settori di competenza. L'inserimento della formula della multiutenza sulla rete intranet in luogo delle autenticazioni basate su credenziali individuali ha permesso di ottimizzare la condivisione delle risorse, riducendo i costi e aumentando il numero delle banche dati giuridiche di accesso web e di accesso remoto rese disponibili su tutte le postazioni dell'Ufficio.

Nel 2013 i documenti richiesti in lettura dagli utenti interni sono stati 4.403 (302 i prestiti), i casi di assistenza bibliografica 102 (33 *online*) e 61 le riproduzioni di documenti con inoltro in formato elettronico (servizio di *Document Delivery*). Le autorizzazioni alla frequentazione degli utenti esterni sono salite a 180 (erano 135 nel 2012), con 2.996 volumi consegnati in lettura (1.906 nel 2012, pari a +57%), 234 casi di assistenza bibliografica (62 *online*) e 402 invii di *Document Delivery* (+74% sul 2012). La consultazione del catalogo OPAC non ha registrato sostanziali variazioni rispetto al 2012 (6.014 contatti contro 6012). I casi di assistenza bibliografica e di *Document Delivery* effettuati *online* sono stati 278 (231 per l'utenza esterna). I dati statistici di consultazione dei *database* giuridici da parte della utenza interna rivestono speciale importanza come indicatori dell'elaborazione che precede la messa a punto dei "prodotti" dell'Ufficio. Per quanto riguarda le quattro banche dati giuridiche di maggiore rilevanza, il numero totale dei documenti consultati nel 2013 ammonta a circa 90.000, con un incremento di circa il 20% sul 2012. Il *database* con il più elevato conteggio statistico ha totalizzato 6.529 sessioni di lavoro (5.828 nel 2012, 4.889 nel 2011 e 4.052 nel 2010), e 75.525 documenti consultati (60.419 nel 2012, 60.141 nel 2011 e 48.112 nel 2010), per una media giornaliera lavorativa di circa 29 connessioni e 337 documenti (26 connessioni e 275 documenti nel 2012).

PAGINA BIANCA

L'Ufficio del Garante

PAGINA BIANCA

III - L'Ufficio del Garante

21 La gestione amministrativa dell'Ufficio

21.1. *Il bilancio e la gestione finanziaria*

Gli importi acquisiti al bilancio del Garante sono stati utilizzati per lo svolgimento dei compiti istituzionali demandati all'Ufficio e per il perseguimento degli obiettivi programmatici definiti in sede di approvazione del bilancio di previsione, nel rispetto delle procedure di legge e regolamentari che disciplinano la materia.

In considerazione della particolare attività svolta a tutela dei diritti fondamentali della persona e dell'ambito (trasversale) di intervento dell'Autorità – non limitabile quindi a specifici "mercati di riferimento" per reperire le risorse finanziarie al fine di contribuire al sostenimento delle proprie esigenze di funzionamento – la parte prevalente delle fonti di finanziamento sono costituite da trasferimenti che il legislatore ha posto a carico di altri soggetti pubblici e dello stesso bilancio statale; solo in misura meno significativa l'Autorità può avvalersi di risorse proprie.

In particolare, la misura più consistente dei fondi complessivamente occorrenti all'Autorità è stata assicurata da altre autorità amministrative indipendenti in misura pari a complessivi 12,0 milioni di euro. A tale proposito, deve tuttavia essere evidenziato che analoga entità di finanziamento annuale è prevista fino al 2016 ma il buon esito del trasferimento dei fondi rischia di essere influenzato, già a partire dal corrente anno, dagli effetti di una recente sentenza del Tribunale amministrativo regionale per il Lazio, sez. II (depositata il 5 marzo 2014), in esito ad un contenzioso sorto tra una delle sei autorità chiamate ad erogare quota parte del contributo ed alcune società operanti nel proprio settore di intervento.

Il menzionato trasferimento è stato previsto da una specifica disposizione contenuta nella legge di stabilità per il 2013 che ha sostanzialmente prorogato una precedente previsione in virtù della quale, a decorrere dal 2011, il Garante ha fruito di un finanziamento annuale di analogo importo volto ad assicurare la gestione corrente e lo svolgimento dei compiti istituzionali.

La stessa legge di stabilità, inoltre, nell'ambito delle previsioni della tabella C, ha stanziato ulteriori somme per un importo di 8,8 milioni di euro, anche se il Ministero dell'economia e delle finanze in corso d'anno ha operato riduzioni per effetto delle quali le somme effettivamente affluite a tale titolo nella disponibilità dell'Autorità sono state pari a 8,4 milioni di euro.

Una parte residuale dei fondi necessari ad assicurare il funzionamento sono derivati, poi, da risorse proprie costituite dalle somme relative a sanzioni riassegnate dall'autorità governativa nonché dai diritti di segreteria riscossi direttamente dall'Ufficio.

La gestione amministrativa ha fatto registrare nell'esercizio in esame entrate in lieve contrazione rispetto all'anno precedente. Lo scostamento, pari a circa 0,5 milioni di euro, è stato determinato in larga misura dal minore trasferimento erariale.

Le entrate totali di cui il Garante ha acquisito il diritto alla riscossione nel 2013 sono state pari complessivamente a 23,0 milioni di euro, il cui importo risulta in lieve flessione rispetto al precedente esercizio nel quale le entrate accertate erano state pari a circa 23,5 milioni di euro.

La parte preponderante degli importi per i quali è maturato nell'anno il diritto all'acquisizione è stata riscossa nell'esercizio di competenza mentre una minima parte degli incassi, per effetto della fisiologica dinamica gestionale, è stata rinviata al corrente esercizio.

Per quanto attiene alle uscite, il confronto dei dati consuntivi dell'esercizio con i valori assunti in sede di stima iniziale hanno evidenziato significative economie alla cui realizzazione si è pervenuti anche per effetto dell'applicazione delle misure di contenimento della spesa previste sul piano legislativo alle quali si sono sommati gli effetti di una attenta gestione in linea con le esigenze di un generale contenimento della spesa.

Gli oneri complessivi imputabili alla competenza dell'esercizio sono stati pari a 18,7 milioni di euro, la cui entità ha fatto registrare un'importante contrazione anche rispetto alla spesa del precedente esercizio finanziario, sia per gli oneri di mero funzionamento, sia per quelli di investimento.

Dal raffronto dell'esercizio 2013 con quello precedente emerge, infatti, una riduzione della spesa complessiva di oltre 1 milione di euro, di cui il 70% circa è imputabile alla gestione corrente mentre la rimanente parte riguarda la minore spesa in conto capitale.

Rispetto alle stime iniziali assunte in sede di previsione annuale, gli oneri effettivamente impegnati hanno fatto registrare una riduzione di oltre 4 milioni di euro alla cui economia hanno concorso principalmente la realizzazione di minori spese di investimento nonché il differimento del completamento della pianta organica.

Tali risultati derivano anche da una specifica scelta gestionale che ha consentito di realizzare nell'anno le economie di spesa in questione, rendendo tali scelte pienamente coerenti con le esigenze delineate in via generale sul piano legislativo.

L'Ufficio, infatti, ha proseguito l'attività di razionalizzazione della spesa cominciata già negli anni immediatamente precedenti, con il sostanziale azzeramento, sia del servizio delle cd. auto blu, lasciando in uso soltanto il veicolo messo a disposizione dalla Guardia di finanza e destinato – in via esclusiva – alle esigenze del Presidente in qualità di alta carica istituzionale, sia delle consulenze a cui l'Ufficio non ha fatto mai ricorso durante tutto l'esercizio. Nel corso dell'anno, poi, si sono registrati gli effetti della dismissione di una estesa superficie immobiliare costituita da un ampio magazzino, utilizzata dall'Ufficio dalla data di istituzione della stessa Autorità e non più indispensabile per il perseguimento delle finalità istituzionali (cfr. Relazione 2012, p. 341).

Esigenze di bilancio, unitamente alla necessità di pervenire ad una contestuale razionalizzazione degli spazi fruibili, hanno indotto l'Ufficio a promuovere la risoluzione del relativo rapporto con la proprietà, i cui effetti finanziari si sono realizzati a carico del bilancio 2013 con una minore spesa corrispondente al relativo canone.

Tali interventi, unitamente ad ulteriori attività di razionalizzazione gestionale, hanno consentito un significativo contenimento della spesa rispetto alle previsioni iniziali.

Per quanto attiene agli emolumenti corrisposti al personale, nell'esercizio si è registrata una diminuzione della spesa, anche se di entità contenuta, le cui ragioni risiedono, da un lato, nei vincoli previsti dalle vigenti disposizioni legislative che, di fatto, impediscono di prevedere incrementi retributivi, e, dall'altro lato, dalla normale dinamica gestionale del personale che ha consentito i pur modesti effetti positivi sul bilancio.

Ciò nonostante la spesa per il personale e per i relativi oneri riflessi, pari al 73% circa delle somme complessivamente impegnate nell'anno, rappresenta la parte più significativa dell'intero bilancio. Peraltro, trattandosi di oneri aventi carattere fisso e continuativo non comprimibili oltre determinati margini per semplice iniziativa dell'amministrazione, non appare possibile prevedere particolari ed ulteriori margini di intervento rispetto a quelli finora già adottati dall'Ufficio.

La rimanente parte della spesa, connessa essenzialmente al funzionamento dell'Ufficio, è stata contenuta entro i limiti previsti dalle disposizioni finanziarie che disciplinano la materia della spesa pubblica.

La spesa per l'acquisizione di beni durevoli, aventi un'utilità pluriennale, ha fatto registrare un'ulteriore ed evidente riduzione, sia rispetto alle previsioni iniziali, sia con riferimento al precedente esercizio, a conferma di un generalizzato criterio di contenimento dei costi che ha indotto il Garante a posticipare il sostenimento di oneri ove nell'immediato non strettamente necessari.

Le finalità istituzionali sono comunque state perseguite e, nonostante le esigenze di bilancio, l'attività amministrativa non ha subito rallentamenti.

La tabella allegata alla presente Relazione (v. sez. IV, tab. 20) riassume sinteticamente la gestione dell'Autorità nel 2013, ponendo a raffronto i valori finanziari di competenza con quelli corrispondenti dell'esercizio precedente.

In particolare, la tabella espone le fonti di finanziamento complessive dell'anno, con evidenziazione degli importi posti a carico del bilancio dello Stato. Per quanto riguarda la spesa, l'onere complessivo sostenuto dall'Ufficio per lo svolgimento delle attività istituzionali trova separata evidenza tra la spesa connessa al funzionamento, comprensiva degli oneri per gli organi e per il personale, e quella per investimento e per rimborsi, nonché per restituzioni in favore del bilancio dello Stato. Accanto ai valori registrati nell'anno sono indicati, per finalità di raffronto, quelli del precedente esercizio, con evidenziazione in apposita colonna degli scostamenti registrati tra i due periodi.

21.2. *L'attività contrattuale e la gestione economale*

L'attività contrattuale dell'Autorità, anche nel 2013, è stata improntata a conseguire, coerentemente con gli indirizzi di carattere generale, i migliori risultati in termini di efficienza e di risparmio: in tale prospettiva, si è giunti pressoché a completare il percorso avviato nel biennio precedente teso, da un lato, ad accorpare le procedure per l'acquisizione di beni e servizi dell'Autorità e, dall'altro, a prolungare la durata dei relativi affidamenti.

L'attività contrattuale ha così registrato una riduzione in termini numerici, consentendo all'Ufficio di concentrarsi sulla definizione di alcuni aspetti che attendevano da tempo adeguata soluzione. Fra questi merita menzionare l'affidamento della gestione integrata delle trasferte di lavoro che, attuata mediante utilizzo dei cd. Accordi quadro della Consip, consentirà una migliore gestione operativa ed un efficace monitoraggio delle esigenze di spostamento per il personale dell'Autorità, il tutto nel quadro di una auspicata riduzione dei costi.

L'utilizzo degli "Accordi quadro", così sperimentato per la prima volta dall'Autorità, non è stata l'unica occasione di ricorso alle procedure Consip. Infatti, con buoni risultati in termini di efficienza operativa e di risparmio, anche nel 2013 è stato fatto costante riferimento alle convenzioni ed utilizzato, ogni qual volta ciò sia risultato possibile, il Mercato elettronico della p.a. (Mepa) tramite richiesta di offerta (RdO) ricorrendo all'acquisto diretto, limitatamente ad importi modesti.

In particolare, sono state utilizzate le convenzioni Consip per la telefonia *mobile* (conv. "Telefonia *mobile* 5"), per l'acquisto di carburante tramite cd. *fuel card* (conv. "Carburanti rete – *fuel card* 5"), per l'approvvigionamento di buoni pasto per il personale (conv. "Buoni pasto 6") nonché per adeguare alcuni aspetti degli atti contrattuali vigenti, destinati alle varie tipologie di manutenzione dell'immobile nell'ambito della convenzione "*Facility management* uffici 3", alle sopravvenute esigenze dell'Autorità.

Per quanto riguarda il Mepa, nel periodo in considerazione, si è ricorsi allo strumento della richiesta di offerta nel 44% del totale delle procedure di gara ed agli affidamenti diretti al miglior offerente nel 9% del totale degli affidamenti.

In merito alle altre procedure, anche nell'anno in considerazione è stata svolta una gara comunitaria per l'acquisizione del servizio di assistenza sanitaria a favore dei dipendenti. Dopo alcuni anni nei quali tali procedure erano andate deserte, si è avuta la partecipazione di un Raggruppamento temporaneo di imprese (Rti) al quale è stato affidato il servizio per un biennio con possibilità di rinnovo annuale.

Sempre con procedura di gara aperta, seppur sotto soglia comunitaria, sono stati affidati altri importanti servizi (rassegna stampa e monitoraggio radio-tv; monitoraggio delle attività delle istituzioni nazionali), con esiti altamente positivi in termini di risparmio per l'Autorità e di razionalizzazione dei servizi.

In ragione dell'urgenza, della maggiore economicità della procedura e, talvolta, in relazione al bene/servizio richiesto, si è ricorsi alla procedura di cottimo fiduciario, con buoni risultati in termini di risparmio rispetto agli importi stabiliti a base d'asta. In particolare, la procedura tesa a determinare il fornitore di una connessione in fibra ottica per la sede dell'Autorità ha determinato un considerevole risparmio, nonché un miglioramento delle prestazioni ottenute rispetto al passato. Si è utilizzato il cottimo fiduciario anche per coprire il periodo di vacanza fra una convenzione Consip e l'altra in materia di buoni pasto, con un ribasso del 15% sulla base d'asta, nonché per la fornitura di banche dati giuridiche che, accorpate in una sola procedura, ha comportato un ribasso pari al 34% sempre sulla base d'asta.

Nel corso dell'anno sono stati poi eseguiti alcuni affidamenti diretti *ex* art. 57, comma 2, lett. *b*), del codice dei contratti pubblici (fornitore unico), in particolare con riferimento ad alcuni prodotti informatici e di agenzie di informazione.

Sono stati infine effettuati, mediante procedura negoziata, numerosi atti di cd. micro-contrattualistica, in relazione ad esigenze di importi esigui.

In relazione all'attività di carattere economale è stata curata la manutenzione ordinaria dell'immobile e degli impianti, con particolare attenzione ai profili della sicurezza e contenendo le spese mediante individuazione prioritaria degli interventi urgenti o indifferibili.

È stata altresì effettuata una rilevante attività di scarto di atti di archivio, che ha consentito lo sgombero di parte dei magazzini acquisiti in modalità di *self storage* e il successivo versamento in essi del materiale d'archivio più datato con evidenti vantaggi in merito all'utilizzo degli spazi della sede.

È stata infine portata a compimento la procedura transattiva con il Dipartimento della protezione civile, legata ai canoni di occupazione del magazzino a suo tempo in uso all'Autorità.

Da segnalare, in ultimo, l'attività di sensibilizzazione e formazione portata avanti dalla struttura che ha organizzato e tenuto appositi incontri per il personale destinato a far parte di commissioni di gara o ad assumere il ruolo di Responsabile unico del procedimento (Rup).

21.3. *Le novità legislative e regolamentari e l'organizzazione dell'Ufficio*

Nel 2013, in coerenza con gli obiettivi di contenimento della spesa pubblica previsti dal d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122, è proseguito un rigoroso processo di *spending review*. In tale quadro, come si è anticipato, anche nel periodo considerato, non sono stati conferiti incarichi di consulenza e sono state ulteriormente contenute le spese per la sola auto di servizio, messa a disposizione dalla Guardia di finanza, e utilizzata per le esigenze di mobilità del Presidente dell'Autorità.

È altresì proseguita la riflessione sul complessivo assetto funzionale e organizzativo dell'Autorità. In tale contesto, è stato avviato un primo processo di avvicendamento dei dirigenti negli incarichi dirigenziali, in occasione del rinnovo degli stessi, ed è stato contestualmente delineato un percorso istituzionale ed amministrativo volto ad introdurre elementi di semplificazione organizzativa e a ridefinire l'ambito di competenza di talune unità organizzative. È stata, inoltre, creata un'unità incaricata di monitorare il processo di elaborazione del nuovo quadro normativo dell'Unione europea in materia di protezione dei dati personali.

Pur nel contesto di una sensibile riduzione dello stanziamento a disposizione dell'Autorità, è stata dispiegata ogni possibile iniziativa per potenziarne l'organico, al fine di un migliore svolgimento delle attività istituzionali. Nel 2013 si è conclusa la procedura di mobilità volontaria esterna, ai sensi dell'art. 30, d.lgs. n. 165/2001, indetta per la qualifica di funzionario con profilo informatico/tecnologico e sono proseguiti i lavori dell'analoga procedura per funzionario con profilo giuridico (conclusa agli inizi di febbraio 2014).

In tale quadro, è da segnalare che la l. 27 dicembre 2013, n. 147 (legge di stabilità 2014), all'art. 1, commi 268 e 269, prevede che al fine di non disperdere la professionalità acquisita dal personale con contratto a tempo determinato, assunto a seguito di procedura selettiva pubblica, nonché per far fronte agli accresciuti compiti derivanti dalla partecipazione alle attività di cooperazione tra le Autorità di protezione dati dell'Unione europea, la consistenza dell'organico del Garante è stato incrementato di dodici unità con contestuale riduzione, nella medesima misura, del contingente di contratti a tempo determinato di cui all'art. 156, comma 5 del Codice. Per le predette finalità, il Garante è stato autorizzato a indire, entro il 31 dicembre 2016, una o più procedure concorsuali per assunzioni a tempo indeterminato di personale in servizio presso l'Ufficio, alla data di entrata in vigore della legge di stabilità, con contratto a tempo determinato che, alla data di pubblicazione del relativo bando, abbia maturato almeno tre anni di anzianità con contratto a tempo determinato. Tali disposizioni, che non prevedono oneri aggiuntivi a carico delle finanza pubblica, si collocano nel solco di quanto previsto per le amministrazioni pubbliche dall'art. 4, comma 6 del d.l. 31 agosto 2013, n. 101, convertito, con modificazioni, dalla l. 30 ottobre 2013, n. 125, e consentiranno un rafforzamento dell'organico dell'Autorità nonché una valorizzazione di professionalità che altrimenti sarebbero andate disperse.

Nel periodo considerato è stato sottoscritto un accordo di collaborazione con l'Agenzia delle entrate il quale prevede che l'Autorità ospiti due funzionari con profilo informatico che saranno impiegati in attività idonee a sviluppare un'esperienza specifica in materia di protezione dei dati personali, con particolare riguardo allo sviluppo dei sistemi informatici per garantire la sicurezza dei dati, anche in vista dell'emanando regolamento europeo in materia.

21.4. *Il personale e i collaboratori esterni*

Nel 2013, a conclusione della procedura di mobilità volontaria esterna per funzionario con profilo informatico/tecnologico, indetta ai sensi dell'art. 30, d.lgs. n. 165/2001, sono stati dichiarati idonei a ricoprire le relative posizioni due funzionari appartenenti ad amministrazioni pubbliche, immessi nel ruolo organico agli inizi del 2014.

Sono state effettuate due assunzioni con contratto a tempo determinato e rinnovato un contratto a termine, sulla base di un accordo negoziale sottoscritto con le rappresentanze sindacali del personale, ai sensi dell'art. 5, comma 4-*bis*, d.lgs. n. 368/2001, con il quale si è convenuto di prevedere la possibilità di un rinnovo quadriennale dei contratti di lavoro in scadenza al fine di assicurare un livello elevato di prestazioni presso le unità organizzative di assegnazione del predetto personale.

Nel periodo considerato l'Autorità ha adeguato la disciplina interna in materia di *stage* alle "Linee guida in materia di tirocini", definite con l'Accordo in sede di Conferenza tra Governo, Regioni e Province autonome di Trento e Bolzano del 24 gennaio 2013 e alla deliberazione n. 199 del 18 luglio 2012 della Giunta regionale della Regione Lazio, con la quale è stata data attuazione al richiamato Accordo, prevedendo una durata non superiore a sei mesi per i tirocini di orientamento e formazione. In conformità a quanto previsto dal citato Accordo, è stato altresì introdotto per la generalità dei datori di lavoro privati e pubblici l'obbligo di corrispondere ai tirocinanti un'indennità mensile di euro 400, già prevista presso il Garante.

Al 31 dicembre 2013 l'Ufficio poteva contare su un organico, a diverso titolo, di centonove unità, di cui centoquattro in servizio, al quale va aggiunto un contingente di personale a contratto di diciotto unità (cfr. tab. 19).

Dai suddetti dati si evidenzia come nell'anno considerato, pur essendosi verificato un incremento dell'organico rispetto all'anno precedente di un'unità, il personale impiegato sia rimasto immutato. Per quanto riguarda la distribuzione del personale per tipologia contrattuale e lavorativa, il dato saliente è rappresentato dal numero di unità di ruolo rispetto al totale, con una percentuale di poco superiore all'ottanta per cento. Tale rapporto dovrebbe migliorare nel 2014 per effetto dell'incremento di organico di dodici unità e della contestuale riduzione, nella medesima misura, del contingente dei contratti a tempo determinato, in attuazione del menzionato art. 1, commi 268 e 269 della l. n. 147/2013.

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 servizi di prevenzione e sicurezza).

Presso l'Autorità opera il servizio di controllo interno che è presieduto da un magistrato della Corte dei conti e composto da due dirigenti generali, rispettivamente, della Ragioneria generale dello Stato e della Presidenza del Consiglio dei Ministri.

21.5. *Il settore informatico e tecnologico*

Sviluppo del sistema informativo e dei servizi ICT

Nel 2013 è proseguita l'attività di sviluppo del sistema informativo nel solco delle direttrici di innovazione tracciate dal Cad, con enfasi sulla smaterializzazione dei flussi documentali e sulla cooperazione interna.

Nell'ambito dell'accordo di collaborazione con il Ministero degli affari esteri per il riuso della piattaforma "documentale@doc", è stata completata l'analisi di alcuni flussi amministrativi relativi a procedimenti a rilevanza esterna o a procedimenti interni. Si è quindi proceduto all'implementazione di due flussi informatici tramite

il sistema di *workflow* acquisito in riuso, con risultati incoraggianti dal punto di vista delle economie raggiungibili come effetto della dematerializzazione della trattazione degli affari di competenza dell'Ufficio.

Nello stesso tempo è stata completata la migrazione dei servizi di posta elettronica interni da piattaforma IMAP/Dovecot a Microsoft Exchange. È stato svolto un accurato *assessment* (Microsoft Exchange RAP) per verificare le *performance* del sistema a regime e sono state risolte alcune criticità relative ai *backup* della posta elettronica.

Sono stati installati certificati digitali di tipo S/MIME per la firma digitale di posta elettronica che, grazie alla procedura formalizzata seguita dall'Ufficio, hanno valenza di firma elettronica avanzata.

È stata completata la nuova rete *WiFi* dell'Ufficio, ottenuta reingegnerizzando l'intera rete preesistente, con l'introduzione di nuovi protocolli di autenticazione volti alla semplificazione dell'interazione degli utenti pur nel rispetto dei più rigorosi *standard* di sicurezza.

È stata potenziata l'area intranet basata sul sistema Microsoft SharePoint, con l'area di supporto della segreteria del Collegio per la gestione documentale delle adunanze del Garante.

Sempre in ambiente SharePoint è stata adottata un'applicazione web per la condivisione di documenti elettronici con collaboratori esterni.

Per quanto attiene ai servizi *cloud*, è stato sperimentato un nuovo sistema di *cloud* privato basato sul *software open source* OwnCloud.

Si è infine provveduto alla creazione del nuovo registro di protocollo per la registrazione di atti e delibere emanati dal segretario generale.

Nell'ambito della manutenzione intesa come mantenimento e accrescimento dei livelli di efficienza delle soluzioni informatiche, è stata installata la versione 4.6 dell'applicativo di protocollo informatico Folium™, con l'arricchimento delle funzionalità e l'integrazione a livello di web *services* con la piattaforma di *workflow* in via di sviluppo.

Il sito web del Garante, reso disponibile al pubblico durante l'ultimo trimestre del 2012, è stato soggetto a manutenzione continuativa, anche con inserimento di nuove funzionalità e l'arricchimento con nuovi contenuti anche di tipo interattivo; tra questi il servizio automatizzato di invio *newsletter* ai cittadini, con la possibilità da parte del cittadino stesso di iscriversi o cancellarsi in autonomia direttamente *online*.

È stata installata una nuova piattaforma gestionale per le risorse umane e per la rilevazione delle presenze, con configurazione web dell'area intranet sicura che permette al personale la visione del proprio cartellino presenze.

È stato predisposto il capitolato tecnico per l'affidamento del servizio telematico di rassegne stampa e di monitoraggio dei flussi di notizie rilevate dai canali radiotelevisivi.

Sono stati inoltre acquistati, installati e configurati nuovi certificati digitali per i *server* web "ssl" con gestione dei *domain name* di tipo *wildcards*.

Dal punto di vista sistemistico, è proseguita l'attività di installazione di sistemi di monitoraggio e gestione del parco macchine, con il ricorso al sistema Nagios e al *software* Cacti.

In vista dell'adozione della nuova Carta Nazionale dei Servizi sono stati svolti alcuni test sull'*Active Directory* relativi alla integrazione delle cd. funzionalità di *smart logon* tramite certificati di autenticazione CNS.

Impegno per la sicurezza informatica dell'Ufficio

Anche nel 2013 nessun incidente informatico di rilievo è occorso nel dominio dell'Ufficio, e in particolare nessun evento relativo alla sicurezza ha prodotto danni o disservizi. Relativamente alla crescente diffusione di virus informatici e del cd. *malware*, sono stati aggiornati gli strumenti di protezione perimetrale e locale che hanno consen-

tito di evitare l'insorgere di inconvenienti. Non si sono registrate perdite di dati e le procedure di *backup* e *recovery* hanno sempre consentito di porre rimedio a occasionali problemi relativi a cancellazioni involontarie o danneggiamento di documenti informatici.

Attività di consulenza e cooperazione interne ed esterne

Il Dipartimento ha collaborato con le altre unità organizzative dell'Ufficio nella trattazione di procedimenti e attività ispettive nonché alle attività internazionali del Garante, in particolare nell'ambito del sottogruppo *technology* del Gruppo Art. 29 (cfr. par. 19.3) e del Gruppo di Berlino (cfr. par. 19.5). Tra le attività più significative si evidenziano la partecipazione all'attività ispettiva nell'ambito del trattamento dei dati dei lavoratori e alle politiche di navigazione internet presso un comune; l'attività ispettiva svolta in vista dell'adozione del provvedimento "Redditometro Agenzia delle entrate"; le attività presso società di recupero crediti; quelle presso fornitori di connettività internet relativa al servizio gratuito di connessione *WiFi*; le ispezioni sul tema del *mobile payment* (nelle due modalità *remote* e *proximity*) con la realizzazione di accertamenti presso operatori, sviluppatori di piattaforme tecnologiche, istituti di credito e gestori di carte di credito.

Relativamente all'attività di consulenza interna, si evidenziano il contributo alla valutazione delle linee guida previste dall'art. 58 del Cad, redatte da DigitPA; l'esame delle convenzioni Inps predisposte sulla base delle citate linee guida; l'analisi del sistema informativo della fiscalità del Ministero dell'economia; l'analisi degli scenari derivanti dalla migrazione delle anagrafi comunali nell'Anagrafe nazionale della popolazione residente (Anpr); la predisposizione di procedure di *audit* da parte del Ministero dell'interno – Direzione N.SIS – in relazione al provvedimento "Schengen" del Garante; il lavoro in tema di deindicizzazione di determinati contenuti di siti web da parte dei motori di ricerca; il contributo alla predisposizione di importanti provvedimenti, quali quelli di *prior checking* legati all'impiego di tecniche di pseudonimizzazione nell'ambito della profilazione dei comportamenti di navigazione degli utenti di internet, nonché all'impiego del canale di ritorno dei servizi di tv interattiva per la profilazione dell'utenza con finalità di *marketing*.

I dati statistici

PAGINA BIANCA

IV - I dati statistici 2013

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	606
Pareri a Presidenza del Consiglio dei Ministri e ministeri (art. 154 del Codice)	22
Autorizzazioni generali al trattamento dei dati sensibili e giudiziari (art. 40 del Codice)	9
Decisioni su ricorso (art. 145 del Codice)	222
Provvedimenti collegiali su segnalazioni e reclami (artt. 142-144 del Codice)	144
Riscontri a segnalazioni, reclami, richieste di pareri e quesiti (artt. 142-144 del Codice e artt. 5 e 11, Reg. Garante n. 1/2007)	4.185
Provvedimenti collegiali su verifiche preliminari per trattamenti che presentano rischi specifici (art. 17 del Codice)	24
Comunicazioni al Garante su flussi di dati tra p.a. o in materia di ricerca scientifica (artt. 19, comma 3, 39 e 110 del Codice)	7
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari	5
Risposte ad atti di sindacato ispettivo e di controllo	4
Risposte a quesiti	31.134
Rilievi formulati in relazione a leggi regionali ai fini dell'impugnazione *ex* art. 127 Cost.	1
Accertamenti e controlli effettuati *in loco* (artt. 157-158 del Codice)	411
Violazioni amministrative contestate	850
Sanzioni applicate con ordinanza di ingiunzione	420
Comunicazioni di notizia di reato all'autorità giudiziaria	71
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	16
Ricorsi (trattati) *ex* art. 152 del Codice	32
Opposizioni (trattate) a provvedimenti del Garante	67
Notificazioni pervenute nell'anno 2013	1.656
Notificazioni pervenute dal 2004 al 31 dicembre 2013	22.683
Riunioni del Gruppo Art. 29	5
Partecipazione a sottogruppi di lavoro - Gruppo Art. 29	32
Riunioni autorità comuni di controllo (Europol, SIS II, Dogane, Eurodac, VIS)	18
Conferenze internazionali	2
Riunioni presso il CoE, OCSE e altri organismi internazionali	12
Riunioni e *workshop* presso Consiglio/Commissione e altri organismi UE	34
Quesiti, questionari e richieste di contributi provenienti da altre Autorità e Istituzioni	52

Tabella 1. Sintesi delle principali attività dell'Autorità

Attività di comunicazione dell'Autorità	
Comunicati stampa	59
Newsletter	15
Dvd (archivio digitale su normativa italiana e attività del Garante)	2
Prodotti editoriali	2
Video divulgativi	4

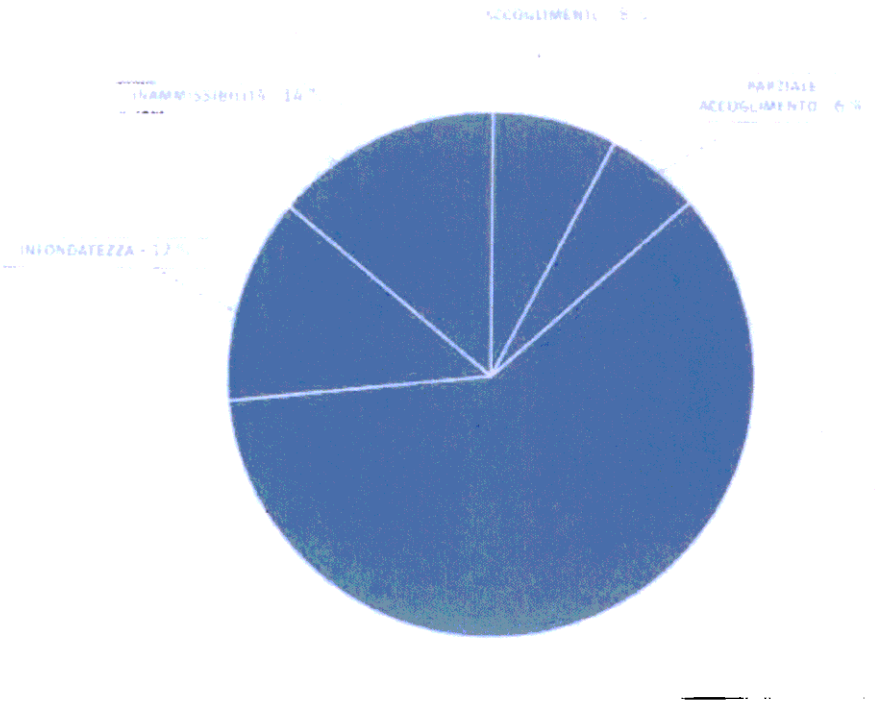
Tabella 2. Attività di comunicazione dell'Autorità

Tabella 3. Pareri *ex* art. 154, comma 4, del Codice

Pareri *ex* art. 154, comma 4, del Codice	
Temi	Riscontri resi nell'anno (*)
Attività di polizia, sicurezza nazionale e governo del territorio	2
Giustizia	1
Informatizzazione e banche dati della p.a.	10
Formazione	3
Tutela della salute e attività sanitaria	1
Attività produttive e professioni	2
Esercizio dei diritti	1
Documenti elettronici	2
Totale	22

Tabella 4. Tipologia delle decisioni su ricorsi

Decisioni su ricorsi	
Tipi di decisione (**)	Numero ricorsi
Accoglimento	17
Parziale accoglimento	13
Non luogo a provvedere (***)	133
Infondatezza	28
Inammissibilità	31
Totale	222



(*) Inerenti anche ad affari pervenuti anteriormente al 2013

(**) 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

Categoria di titolari	Numero ricorsi
Banche e società finanziarie	52
Compagnie di assicurazione	10
Sistemi di informazioni creditizie	15
Società di informazioni commerciali	9
Amministrazioni pubbliche e concessionari di pubblici servizi	19
Strutture sanitarie pubbliche e private	6
Parrocchie	3
Fornitori telefonici e telematici	16
Attività di *marketing* svolta da imprenditori privati	22
Datori di lavoro pubblici e privati	28
Editori (anche televisivi)	22
Amministrazioni condominiali	3
Altri	17
Totale	222

Tabella 5. Suddivisione dei ricorsi in relazione alla categoria di titolari del trattamento

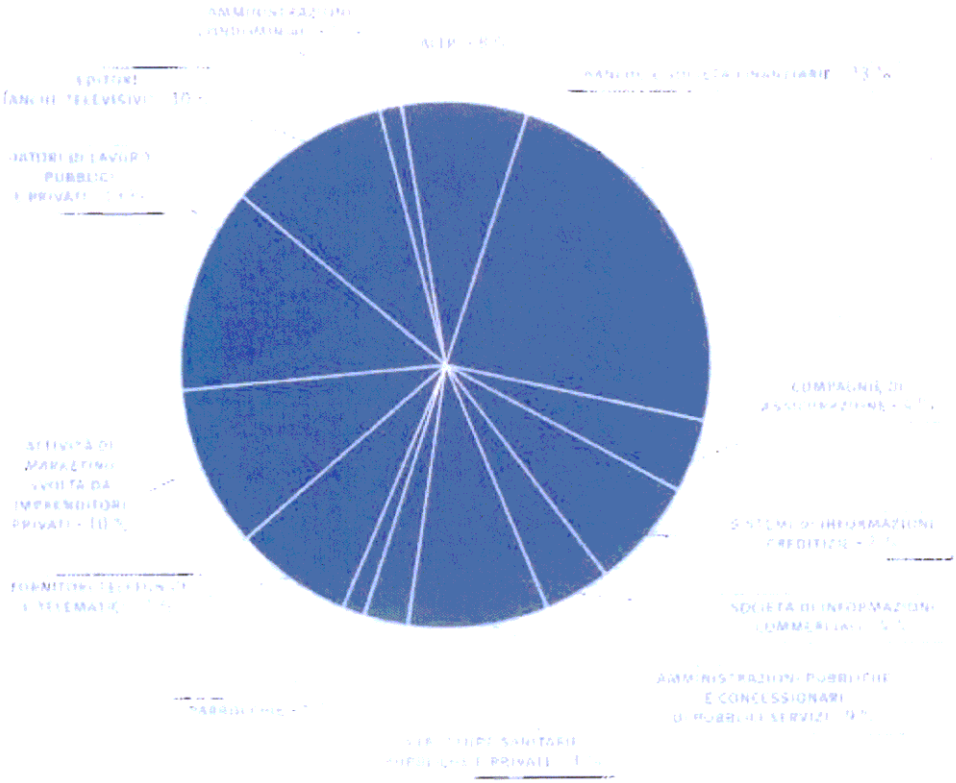
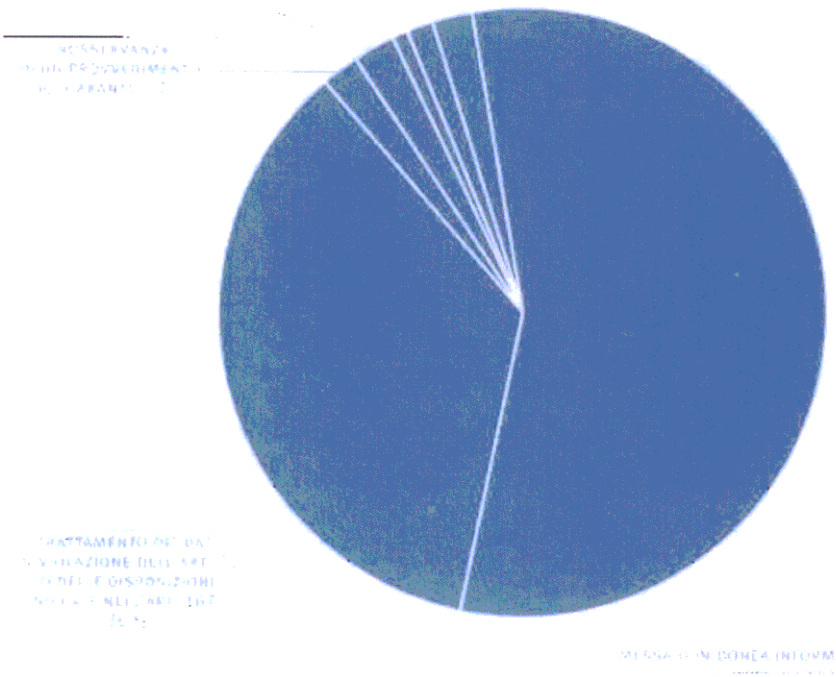


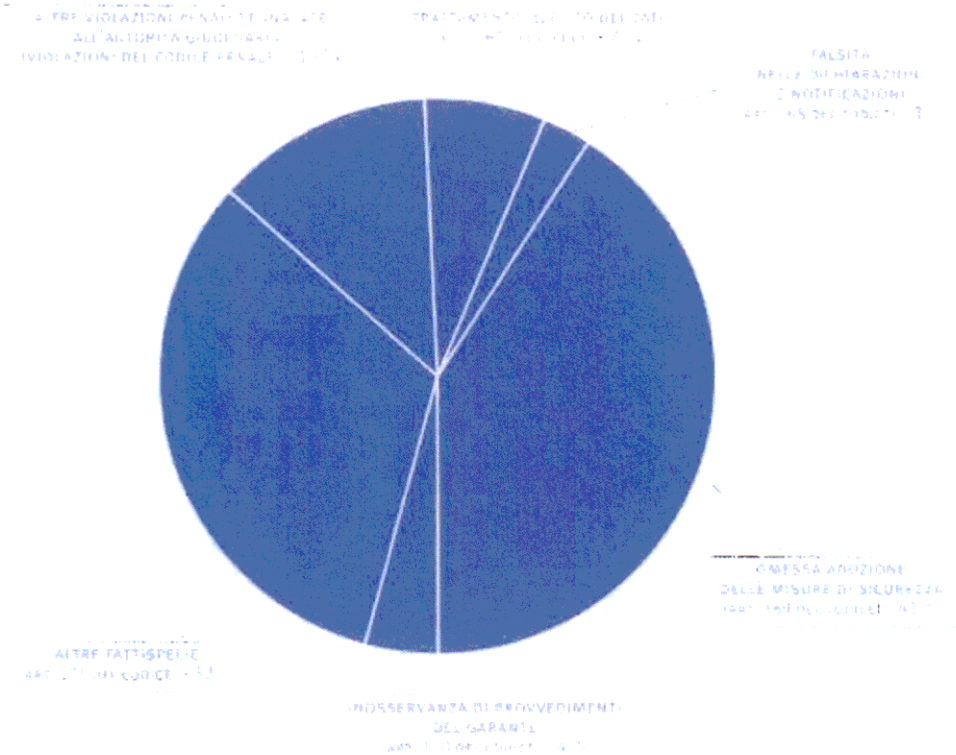
Tabella 6. Violazioni amministrative contestate

Violazioni amministrative contestate	
Omessa o inidonea informativa (art. 161 del Codice)	476
Trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis*, del Codice)	301
Inosservanza di un provvedimento del Garante (art. 162, comma 2-*ter*, del Codice)	17
Violazione del diritto di opposizione (art. 162, comma 2-*quater*, del Codice)	19
Violazioni in materia di conservazione dei dati di traffico (art. 162-*bis* del Codice)	7
Omessa o incompleta notificazione (art. 163 del Codice)	12
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)	18
Più violazioni da parte di soggetti che gestiscono banche dati di particolare rilevanza o dimensioni (art. 164-*bis*, comma 2, del Codice)	-
Totale	850



Comunicazioni di notizia di reato all'autorità giudiziaria	
	Segnalazioni
Trattamento illecito dei dati (art. 167 del Codice)	5
Falsità nelle dichiarazioni e notificazioni (art. 168 del Codice)	2
Omessa adozione delle misure di sicurezza (art. 169 del Codice)	29
Inosservanza di provvedimenti del Garante (art. 170 del Codice)	3
Altre fattispecie (art. 171 del Codice)	23
Altre violazioni penali segnalate all'autorità giudiziaria (violazioni del c.p.)	9
Totale	71

Tabella 7. Comunicazioni di notizia di reato all'autorità giudiziaria



Pagamenti derivanti dall'attività sanzionatoria	
Somme versare a titolo di oblazione in via breve	2.359.868
Somme versate in conseguenza di ordinanze ingiunzione	1.601.892
Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169 del Codice)	120.000
Totale	4.081.760

Tabella 8. Pagamenti derivanti dall'attività sanzionatoria

Tabella 9. Quesiti

Quesiti		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale quesiti	311	216

Tabella 10. Segnalazioni e reclami

Segnalazioni e reclami		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale segnalazioni e reclami	4.393	3.969
Temi principali		
Assicurazioni	112	90
Associazioni	41	44
Centrali rischi	168	169
Concessionari pubblici servizi	86	86
Condominio	30	24
Credito	330	293
Enti locali	87	87
Giornalismo e libertà d'espressione	98	91
Imprese	105	102
Internet	76	71
Istruzione	36	36
Lavoro	377	213
Liberi professionisti	8	8
Marketing	6	7
Recupero crediti	147	88
Sanità e servizi di assistenza sociale	89	89
Telefonia	2.250	2.083
Tributi	5	5
Videosorveglianza	178	177

Tabella 11. Atti di sindacato ispettivo e controllo

Atti di sindacato ispettivo e controllo	
Temi	Numero
Programma PRISM della *National Security Agency* statunitense (NSA)	4
Totale	4

Tabella 12. Tipologie di notificazioni pervenute nel 2013

Tipologie di notificazioni pervenute nel 2013 (**)			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute (1)
Prima notificazione al Garante	23	926	949
Modifica di una precedente notificazione	19	416	435
Notificazione della cessazione del trattamento	5	267	272
Totale	47	1.609	1.656

(*) Inerenti anche ad affari pervenuti anteriormente al 2013

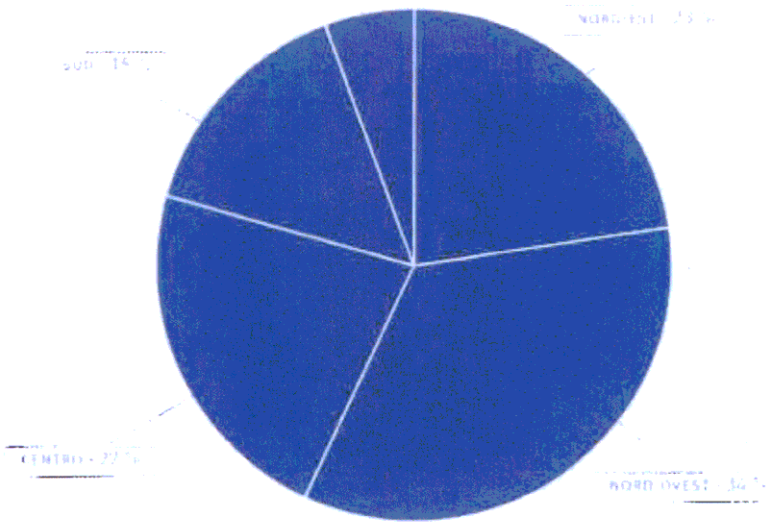
(**) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2013

Tipologie di notificazioni pervenute nel periodo 2004-2013			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute (*)
Prima notificazione al Garante	1.183	17.204	18.387
Modifica di una precedente notificazione	136	3.231	3.367
Notificazione della cessazione del trattamento	72	857	929
Totale	1.391	21.292	22.683

Tabella 13. Tipologie di notificazioni pervenute: 2004-2013

Provenienza geografica delle notificazioni: 2004-2013		
Italia		
Zone geografiche		Pervenute
Nord-Est		5.093
Nord-Ovest		7.755
Centro		5.060
Sud		3.371
Isole		1.268
	Totale	22.547
Da altri Paesi		136

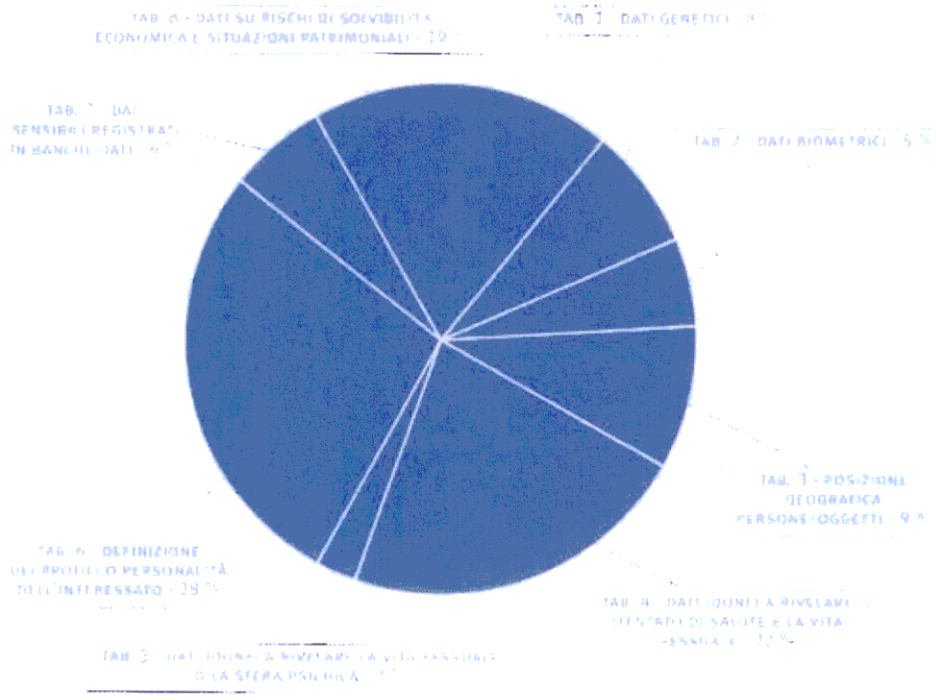
Tabella 14. Provenienza geografica delle notificazioni: 2004-2013



(*) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2013

Tabella 15. Suddivisione delle notificazioni per tipologia di trattamento effettuato: 2004-2013

Suddivisione delle notificazioni per tipologia di trattamento effettuato: 2004-2013	
Tabelle di notificazione compilate (*)	Numero
Tabella 1 - Trattamento di dati genetici	2.492
Tabella 2 - Trattamento di dati biometrici	1.851
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	3.124
Tabella 4 - Trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria	7.199
Tabella 5 - Trattamento di dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale	819
Tabella 6 - Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalita' 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	9.492
Tabella 7 - Trattamento di dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonche' dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie	2.026
Tabella 8 - Trattamento di dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilita' economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti	6.204
Totale	33.207



(*) Situazione alla data del 31 dicembre 2013

Ufficio relazioni con il pubblico	
	2013
E-mail esaminate	17.654
Contatti telefonici	12.800
Persone in visita all'Urp	376
Trattazione pratiche relative a fascicoli	304
Totale	31.134

Tabella 16. Ufficio relazioni con il pubblico

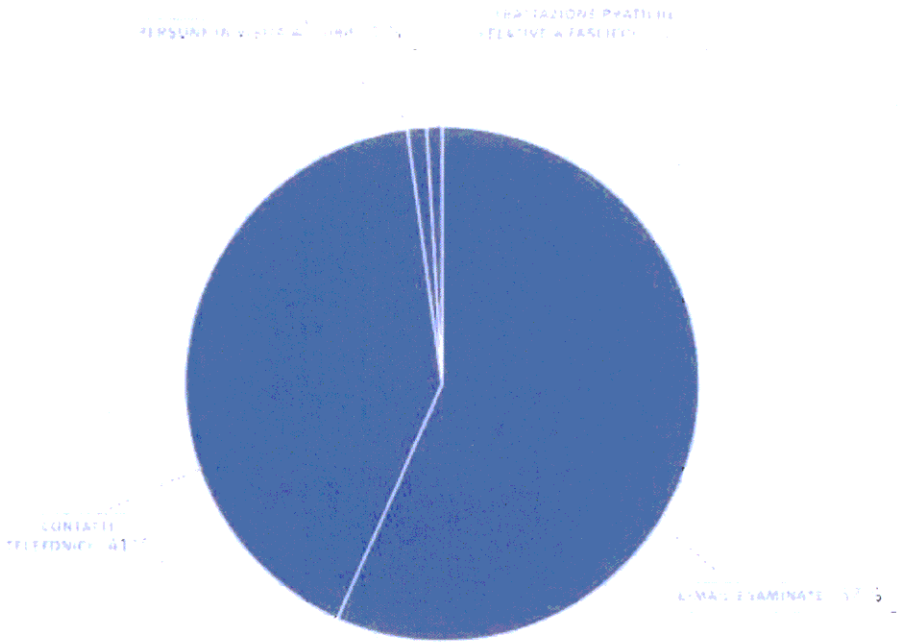


Grafico 17. *E-mail* esaminate dall'Ufficio relazioni con il pubblico (grafico delle categorie)

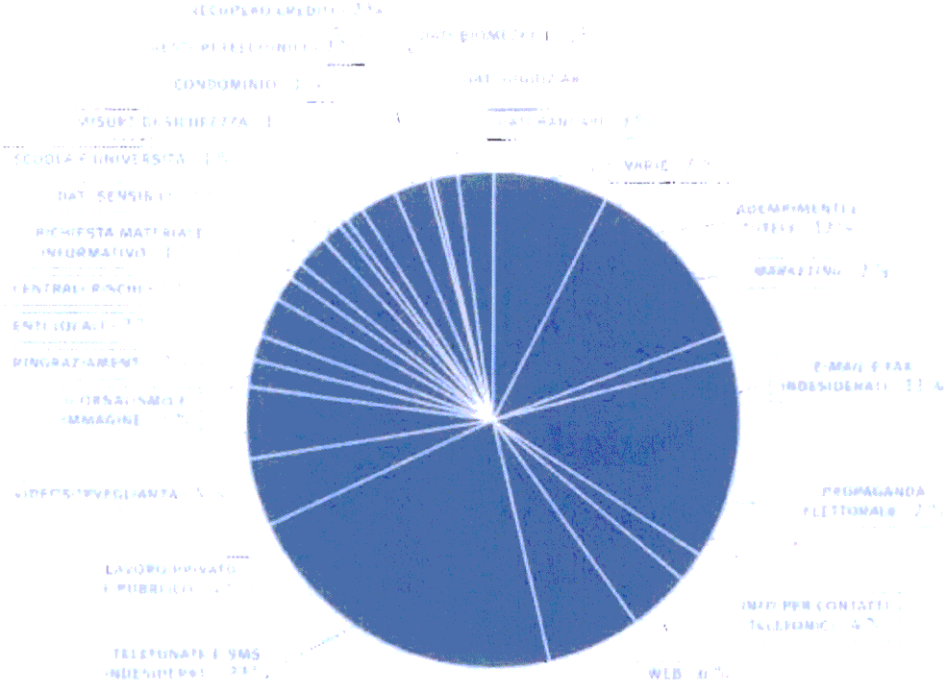


Tabella 18. Posti previsti in organico

Posti previsti in organico	
Segretario generale	1
Dirigenti	24
Funzionari	69
Operativi	30
Esecutivi	1
Totale	125
Personale a contratto	20

Personale in servizio (*)				
Area	In ruolo (a)	In posizione di fuori ruolo (b)	Comandato presso altre aministrazioni o in aspettativa [c]	Impiegato dall'Ufficio (a+b-c)
Segretario generale	1	–	–	1
Dirigenti	14	4	–	18
Funzionari	61	4	5	60
Operativi	25	–	–	25
Esecutivi	–	–	–	–
Totali	101	8	5	104
Personale a contratto				18

Tabella 19. Personale in servizio

Risorse finanziarie			
Entrate accertate	Anno 2013	Anno 2012	Differenza
Entrate correnti	23.029.146	23.571.012	-541.866
di cui trasferimento dallo Stato	8.379.264	8.856.462	-477.198
Totale entrate	23.029.146	23.571.012	-541.866
Spese impegnate	Anno 2013	Anno 2012	Differenza
Spese di funzionamento	18.389.709	19.117.292	-727.583
Spese in conto capitale	26.992	338.847	-311.855
Rimborsi al Mef	253.611	251.735	1.876
Totale spese	18.670.312	19.707.874	-1.037.562

Tabella 20. Risorse finanziarie

Tabella 21. Attività internazionali dell'Autorità

Unione europea			
Gruppo Articolo 29	Sessione plenaria Art. 29		26 e 27 febbraio 16 aprile 5 e 6 giugno 2 e 3 ottobre 3 e 4 dicembre
	Riunioni dei sottogruppi	*Border Travel Law Enforcement* (BTLE)	7 e 8 gennaio 14 marzo 23 maggio 4 e 5 luglio 16 e 17 settembre 21 novembre
		E-Government	8 febbraio 3 aprile 16 maggio 11 luglio 31 ottobre
		Financial Matters	14 febbraio 4 aprile 18 settembre
		Future of Privacy	20 febbraio 10 aprile
		International Transfers	7 novembre
		Key Provisions	24 gennaio 30 aprile 25 giugno 19 settembre 15 novembre 12 dicembre
		Technology	29 e 30 gennaio 25 e 26 marzo 21 e 22 maggio 23 maggio *(conference call)* 27 giugno 4 e 5 settembre 5 e 6 novembre
		Google Privacy Policy Task Force	14 maggio 18 giugno *(conference call)* 30 settembre *(conference call)* 4 novembre *(conference call)* 26 novembre *(conference call)* 16 dicembre *(conference call)*
		Training BCR	14 e 15 novembre
		WADA	7 febbraio

Unione europea	
Autorità di controllo comune EUROPOL	4/8 marzo - ispezione 13 marzo 18 marzo 29 aprile "JSB Working Group Europol Regulation" 29 e 30 maggio, Sottogruppo "Europol New Project Group" 10 giugno 9 ottobre 27 e 28 novembre, Sottogruppo "Europol New Projecr Group" 10 dicembre
Autorità di controllo comune EUROJUST	4/6 febbraio - ispezione
Autorità di controllo comune DOGANE	19 marzo 11 giugno 11 novembre 11 dicembre
Gruppo di coordinamento della supervisione SID	11 giugno 11 dicembre
Autorità di controllo comune SCHENGEN	19 marzo
Gruppo di coordinamento della supervisione SIS II	11 giugno 17 ottobre
Gruppo di coordinamento della supervisione EURODAC	12 aprile 16 ottobre
Gruppo di coordinamento della supervisione VIS	11 aprile 16 ottobre

Unione europea		
Riunioni di gruppi di esperti	Consiglio UE - Dapix (Regolamento)	8 e 9 gennaio 21 gennaio 29 e 30 gennaio 12 e 13 febbraio 13 e 14 marzo 27 marzo 9/11 aprile 24 aprile 29 e 30 aprile 13/15 maggio 14 giugno 3 e 4 luglio 22 e 23 luglio 9 e 10 settembre 23 e 24 settembre 17 e 18 ottobre 28 e 29 ottobre 11 e 12 novembre 20 novembre
	Consiglio UE - Dapix (Direttiva)	21 febbraio 24 maggio 4 ottobre 10 dicembre
	Consiglio UE - *Friends of Presidency*	10 gennaio 31 gennaio 14 febbraio 12 marzo
	Commissione UE - *Data Retention*	10 ottobre 17 dicembre
Meeting "Advance Passenger Information"		11 marzo
Meeting of all national authorities competent for personal data breach notifications under the ePrivacy Directive		18 settembre

Altri *forum* internazionali		
Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	Comitato *"Working Party on Information Security and Privacy"*	17 gennaio *(conference call)* 8/10 aprile - Plenaria 6 e 7 giugno - *Expert Group Security Guidelines* 20 novembre *(conference call)* 11/13 dicembre - Plenaria
Consiglio d'Europa	Plenaria	15/18 ottobre
	Comitato T-PD *Bureau*	5/7 febbraio 28/30 maggio 18/20 dicembre
	CAHDATA	12/14 novembre
Gruppi di lavoro specifici	Gruppo internazionale di lavoro sulla protezione dei dati nelle telecomunicazioni (IWGDPT)	15 e 16 aprile 2 e 3 settembre
	Accountability Project	20 e 21 febbraio 6/10 maggio
International Enforcement	IECWG *(International Enforcement Coordination Working Group)*	29 aprile *(conference call)* 28 maggio *(conference call)* 11 settembre *(conference call)*
	Progetto PHAEDRA	17 giugno *(conference call)*
	GPEN *(Global Privacy Enforcement Network – Sweep)*	3 dicembre *(conference call)*

Conferenze internazionali	
Conferenza di primavera delle Autorità europee di protezione dati	15/17 maggio, Lisbona
35ª Conferenza internazionale delle Autorità di protezione dati	23/27 settembre, Varsavia

Altre conferenze	
International Symposium "Open Data - Complementary Concept or Restriction of Freedom of Information?"	27 maggio, Potsdam
Octopus Conference - Cooperation Against Cybercrime	4/6 dicembre, Strasburgo
Conferenza sulle relazioni tra Consiglio d'Europa, Unione europea e Stati membri	15 novembre, Vienna

PAGINA BIANCA

€ 13,40

Stampato su carta riciclata ecologica

171360003360