SENATO DELLA REPUBBLICA

XVII LEGISLATURA

Doc. CXXXVI
n. 3

RELAZIONE

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

(ANNO 2014)

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

Presentata dal Garante per la protezione dei dati personali

(SORO)

Comunicata alla Presidenza il 16 dicembre 2015

TIPOGRAFIA DEL SENATO

INDICE

Signor Presidente della Repubblica,

Signora Presidente della Camera,

Autorità, Signore e Signori,

L'importanza strategica della protezione dei dati

Il progresso e l'innovazione hanno profondamente modificato i nostri modi di vivere, di abitare il mondo, di organizzarlo.

Non solo per le trasformazioni evidenti nei sistemi di comunicazione ma per quelle ancora più rilevanti nelle relazioni economiche, con lo sviluppo dell'economia digitale fondata sui dati, che ridisegna una geografia globale del potere.

Sono cresciute imprese capaci di sconvolgere i meccanismi consolidati della concorrenza, di concentrare nella loro disponibilità tutto il sapere che sette miliardi di persone, individualmente, generano ogni giorno.

È lo sviluppo esponenziale dei Big data, alimentato dall'uso intensivo di tecniche di calcolo sempre più raffinate e precise.

È l'Internet delle cose, con le sue molteplici applicazioni, dalla domotica alle tecnologie indossabili, che attribuisce anche agli oggetti di uso comune un'identità digitale.

È il "pianeta connesso", nuova dimensione delle nostre esistenze che raccoglie non solo le tracce lasciate dal web, ma anche dai geolocalizzatori, dai droni, dai dispositivi intelligenti che elaborano, in tempo reale, perfino dati emotivi e dinamici.

In questa rete pervasiva di oggetti, che interagiscono e comunicano costantemente, l'uomo rischia davvero di ridursi ad un supporto: da analizzare e osservare nei comportamenti, da profilare per condizionarne le scelte,

da sorvegliare per realizzare un controllo sempre più invasivo che di fatto si estende alle nostre abitazioni, alla nostra fisicità.

Tutto ruota intorno ad una raccolta onnivora di dati.

Ma nella società digitale noi siamo i nostri dati e la vulnerabilità dei dati è vulnerabilità delle nostre persone: da questa considerazione si deve partire per ricercare nuove e più efficaci forme di tutela delle nostre libertà.

Ad essere analizzate, sezionate ed elaborate sono oggi le nostre identità affidate ad algoritmi che orientano non solo settori rilevanti dell'economia, della politica, della finanza, ma sempre di più le nostre scelte quotidiane.

Dalla telemedicina alle consultazioni politiche on-line; dalla giustizia telematica al fascicolo sanitario elettronico; dalla videosorveglianza ai social network alle applicazioni per il *live streaming* come *Periscope*; dalla stampa on-line all'analisi genetica del crimine.

Non c'è dimensione della vita, privata e pubblica, che non presupponga un trattamento di dati personali e non richieda solide garanzie per evitare che quei dati vengano usati "contro di noi", privandoci della nostra libertà anziché agevolandone l'esercizio.

Questo mutamento profondo nell'organizzazione della vita quotidiana stimola interrogativi e inquietudini, mette in luce le contraddizioni legate alla pluralità di dimensioni in cui la vita reale si svolge, ripropone il tema delicato del rapporto tra uomo e macchina, il timore represso che l'intelligenza artificiale possa autonomizzarsi dall'uomo e insieme la tentazione di delegare alle tecnologie scelte e decisioni che all'uomo competono.

Gli scenari della società digitale disegnano un quadro di grandi sfide che abbiamo il dovere di affrontare senza rassegnata subalternità e senza inutile ostilità.

Dobbiamo rimuovere la tentazione tecnofobica, il timore dell'innovazione, senza rinunciare a contrastarne le distorsioni, a ricercare una qualche regolazione dei processi e, più in generale, a vivere responsabilmente il nostro tempo.

In questo quadro la protezione dei dati si pone non solo come diritto confinato alla sfera dell'intimità, ma come insostituibile chiave per mantenere l'equilibrio tra fattibilità tecnica ed accettabilità giuridica, tra etica e progresso, presupposto per l'esercizio delle altre libertà.

È utile registrare come non solo la Cassazione ma anche l'ONU, con singolare sincronia, abbiano recentemente sancito il principio che i diritti devono godere on-line della stessa tutela accordata off-line e che l'identità digitale non è meno "personale" di quella reale.

In questa cornice di cambiamenti si dispiega l'attività del Garante.

Per un'informatizzazione della Pubblica Amministrazione attenta al valore dei dati personali

La vulnerabilità di dati non protetti ha effetti dirompenti sulla loro integrità, correttezza e disponibilità.

Non c'è protezione dei dati senza sicurezza e garantire la sicurezza è sempre più difficile, considerato l'aumento esponenziale della criminalità informatica, di cui tutti siamo potenziali vittime: dai furti di identità, di *account* personali, dei sistemi di pagamento elettronico fino ai blocchi di computer con finalità estorsiva.

La prima sfida per l'Autorità è quella di promuovere, nel pubblico e nel privato, un approccio sistematico alla protezione dei dati e delle infrastrutture.

Nella pubblica amministrazione digitale, la sicurezza è un obiettivo chiave per costruire la fiducia dei cittadini e per garantire efficienza e trasparenza.

L'attività del Garante si è articolata nella verifica e prescrizione di misure di sicurezza, relative ai sistemi di archiviazione, ai flussi dei dati, alla interoperabilità delle banche dati condivise tra le amministrazioni dello Stato, gli enti locali, gli organismi di previdenza, le varie agenzie.

I numerosi provvedimenti adottati, spesso all'esito di accertamenti ispettivi, sono stati il frutto di una proficua attività di collaborazione con le amministrazioni che hanno abitualmente recepito le nostre indicazioni.

Un notevole impegno abbiamo profuso per aumentare il livello di sicurezza dello SPID — sistema pubblico utilizzato per gestire le identità digitali — destinato a diventare vera e propria infrastruttura critica, dalla cui efficienza e affidabilità dipenderà la possibilità di fruire di servizi on-line con piena fiducia da parte dei cittadini.

Anche la realizzazione di un moderno ed efficiente sistema fiscale passa per la creazione di nuove banche dati e per l'implementazione e l'interconnessione di quelle esistenti.

Numerosi sono i pareri resi all'amministrazione finanziaria e, tra quelli più recenti, i correttivi richiesti ed introdotti dall'Agenzia delle entrate sul modello 730 precompilato che hanno consentito di individuare modalità tecniche per garantire accessi sicuri, tracciabili e selezionati ai dati dei contribuenti.

Ugualmente nel settore sanitario: la conservazione digitale della cartella clinica, la refertazione on-line, il fascicolo sanitario ed il dossier sanitario sono alcuni dei nostri principali interventi.

E dove è stata accertata, nell'ambito delle numerose istruttorie svolte, l'inadeguatezza dei sistemi, sono stati adottati specifici provvedimenti di blocco, come nel caso di alcune importanti aziende ospedaliere.

L'innovazione tecnologica deve necessariamente essere accompagnata da sistemi di sicurezza informatica che garantiscano autenticazione dei dati, la loro tracciabilità, accessi selettivi con credenziali univoche, cifratura, sistemi di alert e attività di auditing: queste sono alcune delle principali aree di intervento dell'Autorità nell'effettuare le valutazioni con riferimento a tutti gli ambiziosi progetti di modernizzazione dell'Italia.

E per combattere le nuove vulnerabilità della società digitale.

Che si aggiungono alle vecchie e non meno delicate: penso ad esempio al malato di HIV che deve chiedere l'esenzione allo sportello della Asl in cui lavora, o allo studente che ha cambiato sesso e deve esibire il certificato di laurea o al caso controverso dell'anonimato materno.

Per una protezione dei dati davvero dinamica e funzionale

Avvertiamo la responsabilità di rendere effettivi i princìpi del nostro Codice superando, ove possibile, informative dispersive, prescrivendo soluzioni compatibili con la realtà.

Abbiamo consolidato percorsi virtuosi di confronto con gli operatori per definire regole condivise e tecnicamente implementabili.

Rispetto alle rigide soluzioni che rendono di fatto le norme inattuabili abbiamo ricercato forme nuove, come per i *cookie* e il *mobile payment* che, senza ostacolare le esperienze degli utenti, ne richiedono una consapevole interazione.

La semplificazione deve però essere sempre accompagnata da serie politiche di trasparenza.

È nostro impegno costante impedire lo sfruttamento dei dati dei consumatori senza peraltro sottovalutare le esigenze del mercato, come nel parere reso al Ministero dell'economia sul sistema di prevenzione dei furti di identità nel settore del credito al consumo.

Nei rapporti di lavoro il crescente ricorso alle tecnologie nell'organizzazione aziendale, i diffusi sistemi di geolocalizzazione e telecamere intelligenti hanno sfumato la linea – un tempo netta – tra vita privata e lavorativa.

È auspicabile che il decreto legislativo all'esame delle Camere sappia ordinare i cambiamenti resi possibili dalle innovazioni in una cornice di garanzie che impediscano forme ingiustificate e invasive di controllo.

Occorre sempre di più coniugare l'esigenza di efficienza delle imprese con la tutela dei diritti: obiettivo che ha ispirato le decisioni dell'Autorità nelle numerose verifiche preliminari nonché nelle linee guida in materia di biometria.

Nel settore privato, abbiamo avviato puntuali accertamenti per verificare il rispetto delle prescrizioni, a suo tempo impartite alle banche, al fine di innalzare i livelli di sicurezza dei sistemi e dei dati dei correntisti.

La sicurezza del resto ha un ruolo centrale nel nuovo Regolamento UE – giunto alla fase finale – che spinge, tra l'altro, verso l'adozione di modelli che

incorporano la sicurezza dei dati direttamente nelle tecnologie, promuove valutazioni di impatto ed analisi dei rischi ed assegna alle Autorità nuovi e rilevanti compiti come nel caso dei sistemi di certificazioni europee.

La protezione dei dati bussola nel futuro digitale

L'economia digitale ha favorito una concentrazione di potere in mano a piattaforme tecnologiche sempre più esclusive e protagoniste influenti delle relazioni internazionali.

E tuttavia, a partire dalle sentenze della Corte di giustizia, si è aperta una fase nuova.

Il Parlamento europeo, nel novembre 2014, ha approvato una Risoluzione che punta a separare l'attività dei motori di ricerca dagli altri servizi e la Commissione ha aperto una procedura di infrazione per presunto abuso di posizione dominante di Google.

Sono segnali importanti, un freno reale al dilagare senza condizioni del potere delle piattaforme, anche se l'Europa non può ignorare la propria responsabilità per il grave ritardo nella costruzione di un mercato digitale davvero competitivo, prima causa della sua dipendenza tecnologica.

Da tempo la nostra Autorità lavora con l'obiettivo di rimuovere l'asimmetria informativa e l'opacità dei soggetti che dominano il mercato digitale.

Il nostro provvedimento prescrittivo nei confronti di Google punta ad imporre al gigante di internet le stesse regole cui sono tenute le imprese europee.

E il protocollo di intesa sottoscritto, il primo in Europa, assoggetta l'azienda a verifiche periodiche presso la sede californiana (la prima si è svolta a maggio) per monitorare il rispetto delle nostre prescrizioni ma, insieme, permette un confronto costruttivo e dialogante su temi normalmente oggetto di riserbo assoluto da parte della società americana.

La procedura per un corretto esercizio del diritto all'oblio è stata incardinata e costringe i motori di ricerca a porsi come nostri interlocutori spingendoli a

confrontarsi con problematiche complesse che non trovano soluzione soltanto nella tecnologia.

In questo primo anno le richieste di oblio sono state respinte nel 73% dei casi, secondo criteri e valutazioni che il Garante, adito successivamente al rigetto, ha generalmente condiviso.

Abbiamo tracciato un sentiero, dimostrando come la protezione dei dati possa davvero essere la chiave attraverso la quale presidiare le complessità dello spazio digitale.

In questo senso vorrei ricordare il parere sul Programma statistico nazionale, che prevede la possibilità di utilizzare per la prima volta anche i Big data o la consultazione attualmente aperta sull'Internet delle cose o gli accertamenti avviati – a livello internazionale – con riguardo al complesso mondo delle applicazioni, in particolare quelle che offrono servizi ai minori o consentono di monitorare la nostra salute.

Siamo immersi nella società digitale e sempre di più conosciamo noi stessi, il mondo e gli altri attraverso la tecnologia, senza disporre dei necessari anticorpi.

C'è bisogno di una nuova "alfabetizzazione" che promuova comportamenti attivi e informati per gestire con prudenza i nostri dati e, dunque, anche l'approccio divulgativo diventa parte essenziale dei compiti dell'Autorità.

Tutte le Istituzioni sono chiamate ad un supplemento di impegno per ridurre e cancellare la distanza che separa la tutela dei cittadini nello spazio digitale rispetto a quelle consolidate e garantite nello spazio fisico.

Come è stato per la cultura ambientalista, occorre infatti diffondere la consapevolezza che anche nell'Infosfera ogni atto compiuto deve essere un atto responsabile e che il contributo di ciascuno, oggi, è indispensabile per migliorare la prospettiva del nostro futuro e tracciare uno sviluppo sostenibile del pianeta connesso. E questa è sfida che interroga gli Stati ed esige una risposta globale.

Una Kyoto della protezione dati.

Privacy e sicurezza: sinergia, non antitesi

La dimensione digitale sarà sempre più il teatro dei conflitti internazionali.

Il Datagate ha mostrato sia l'insostenibilità democratica sia la sostanziale inefficacia della legislazione emergenziale fondata sulla raccolta generalizzata e indiscriminata delle comunicazioni, con un'inaccettabile quanto inutile compressione del diritto alla privacy.

Quell'esperienza ha indotto gli Usa a orientarsi verso il modello europeo di bilanciamento tra libertà e sicurezza, ben espresso dalla Corte costituzionale tedesca: "la Costituzione esclude il perseguimento della sicurezza assoluta al prezzo della libertà".

Eppure, mentre negli Usa cresce l'adesione a questo modello l'Europa, nella percezione della propria fragilità, rischia di rinnegare se stessa. Come smarrita davanti alla crescente asimmetria che il diritto presenta rispetto a una tecnologia in continua evoluzione e, insieme, alle pulsioni securitarie dell'opinione pubblica.

Ne abbiamo colto un segnale nelle leggi approvate in questi mesi in Spagna e Francia.

E nel percorso del nostro decreto anti-terrorismo.

In fase di conversione, a quel provvedimento – sul cui testo originario siamo stati auditi dalla Camera, oltre che dal Csm – sono state aggiunte una serie di previsioni che – l'abbiamo segnalato – avrebbero alterato il giusto equilibrio tra privacy e sicurezza, sottovalutando anche le implicazioni di alcune tecnologie.

Come nel caso delle intercettazioni da remoto, con il rischio di un serio ostacolo al controllo di legittimità sui dati acquisiti.

È stato un atto di saggezza sia lo stralcio di questa norma sia le opportune modifiche apportate alle previsioni che, da un lato, ammettevano le intercettazioni preventive per qualsiasi reato commesso on-line e che, dall'altro, estendevano "a regime", in misura rilevante e non selettiva il tempo di conservazione dei dati di traffico.

Questo, in palese contrasto con le indicazioni fornite dalla Corte di giustizia

che, con la sentenza sulla data retention, ha sancito la centralità del diritto alla privacy nel suo rapporto con la sicurezza.

Centralità riaffermata poi, con la sentenza sull'oblio (*Costeja c. Google*) rispetto agli interessi economici dei motori di ricerca.

Sentenze coeve a quella della Corte suprema americana che, estendendo alle perquisizioni dei cellulari le garanzie previste per le limitazioni della libertà personale, ha delineato un parallelismo molto più che simbolico tra corpo fisico e corpo elettronico.

Intelligence strategica e sorveglianza di massa

Queste tre pronunce hanno in comune la qualificazione della protezione dati come principale presupposto di libertà nell'era digitale: diritto d'"inviolata personalità" senza il quale ogni democrazia rischia di cedere alla logica totalitaria dell'uomo di vetro e la rete di ridursi a dimensione anomica in cui globalizzare non le libertà, ma l'indifferenza ai diritti.

Dobbiamo contrastare la ricorrente tentazione di considerare le libertà civili come un lusso che non ci possiamo permettere di fronte alla minaccia terroristica.

È dalla centralità dell'*Habeas data* nelle nostre democrazie che deve partire l'Europa per combattere il terrorismo e ogni fondamentalismo senza rinnegare se stessa e la propria identità.

Rivedendo il rapporto tra privacy e sicurezza anche sotto il profilo della reale efficacia della sorveglianza di massa, rivelatasi assai meno utile, anche in termini investigativi, rispetto a quella "tradizionale", mirata e selettiva, come ha dimostrato la Commissione di esperti istituita da Obama.

Il modo migliore per difendere la nostra sicurezza è proteggere i nostri dati – e, con essi, le infrastrutture e i sistemi cui li affidiamo – ed evitarne raccolte massive, limitando "la superficie d'attacco" per un terrorismo che sempre più si alimenta della rete per passare dallo spionaggio informatico alla concretissima violenza delle stragi.

Un'efficace prevenzione del terrorismo dovrebbe dunque selezionare – con intelligenza, appunto – gli obiettivi "sensibili" in funzione del loro grado di rischio e fare della protezione dati una condizione strutturale di difesa dalla minaccia cibernetica, come abbiamo sottolineato anche al Comitato Schengen.

È quanto abbiamo più volte sostenuto, in primo luogo rispetto all'attività d'intelligence, soprattutto strategica che, come ha segnalato il Consiglio d'Europa, ha un raggio di azione assai più ampio e meno "puntuale" di quella tradizionale, suscettibile quindi di degenerare – se non limitato ad obiettivi realmente "sensibili" – in sorveglianza massiva.

In questo senso è particolarmente importante l'avvio di procedure informative specifiche instaurate con il Dipartimento delle informazioni per la sicurezza (Dis), al fine di assicurare la piena conformità al Codice dei trattamenti svolti dalle Agenzie di intelligence e, in tale ambito, i pareri resi quest'anno sulla disciplina delle misure di sicurezza adottate da tali organi.

Ma rischi analoghi di "sovra-acquisizione di dati" possono derivare, sia pure in misura diversa, anche dall'uso di mezzi di ricerca della prova particolarmente invasivi – ad esempio acquisizioni di tabulati o intercettazioni – se non circondati da misure di sicurezza idonee a impedire abusi o non adeguatamente circoscritti sulla base dei presupposti individualizzanti previsti dal codice di procedura penale, con il rischio di trasformarsi, così, da individuali a massivi.

Peraltro, i dati personali acquisiti con questi mezzi investigativi (ed altri: si pensi al prelievo del DNA, i cui profili confluiranno nella banca dati nazionale), vanno protetti anche successivamente alla raccolta, per impedire ogni tipo di abuso.

In tal senso vorrei sollecitare l'urgente attuazione delle misure prescritte, in particolare, al Ministero dell'interno e alle Procure della Repubblica, per garantire la sicurezza dei dati trattati nell'ambito delle rispettive funzioni.

Di questa complessiva "messa in sicurezza" dei centri, privati e pubblici, di raccolta dei dati personali, fa parte anche l'iniziativa del Garante di indicare – all'esito di attività ispettive – specifiche misure ai gestori dei principali

Nodi d'interscambio internet (IXP), per evitare che la fase di instradamento del traffico di dati verso i provider costituisca una zona "franca" e come tale vulnerabile rispetto a ogni tipo di abuso.

Che rispetto a queste strutture avrebbe effetti devastanti.

L'esperienza, anche recente, di altri Paesi europei ci rivela che questi abusi sono possibili anche in ordinamenti democratici (intercettazione dati in Germania presso il *Neutral Exchange Point* di Francoforte, 2015).

Per una trasparenza davvero democratica

Il d.lgs. 14 marzo 2013, n. 33 ha dato un importante contributo per superare la segretezza quale principale forma di esercizio del potere, mutando anche il rapporto tra singolo e autorità: da autoritativo, burocratico e insindacabile a paritetico, partecipato e "controllabile".

Tuttavia, la sua applicazione ne ha mostrato alcune criticità, legate essenzialmente al carattere indifferenziato degli obblighi di pubblicità.

Essi si applicano infatti, con analogo contenuto, ad enti e realtà profondamente diversi tra loro, senza distinzione in ragione del grado di esposizione dell'organo al rischio corruttivo; dell'ambito di esercizio della relativa azione o, comunque, delle risorse pubbliche assegnate, della cui gestione l'ente debba quindi rispondere.

Nel regolare così, in modo identico, situazioni diverse, tali norme rischiano di pregiudicare l'equilibrio complessivo della disciplina, con effetti in larga parte disfunzionali rispetto alla stessa esigenza di consentire "forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche" (art. 1, c. 1, d.lgs. 33/2013).

Pertanto, le limitazioni – spesso significative – della riservatezza, che tali obblighi di pubblicità comportano, possono risultare in alcuni casi irragionevoli e, come tali, meritevoli di revisione.

Del resto, proprio perché strumento di partecipazione, responsabilità

e legittimità, la trasparenza deve essere preservata da effetti distorsivi e da quell'"opacità per confusione" che rischia di caratterizzarla se degenera in un'indiscriminata bulimia di pubblicità.

Con il rischio di occultare informazioni realmente significative con altre inutili, così ostacolando, anziché agevolare, il controllo diffuso sull'esercizio del potere.

Quello dell'opacità per confusione è un rischio in qualche modo implicito nell'approccio scelto dal legislatore italiano, che diversamente dal Foia (*Freedom of Information Act*) ha considerato la divulgazione indiscriminata in rete quale unica modalità di assolvimento degli obblighi di pubblicità.

Va dunque ripensato non il principio di trasparenza come forma ineludibile dell'agire amministrativo, ma le modalità della sua realizzazione, anche seguendo, almeno in parte, il modello del Foia – fondato sulla legittimazione di chiunque ad accedere agli atti amministrativi su istanza di parte – e ridisegnando ambito oggettivo e contenuto degli obblighi di pubblicità, in funzione della loro reale utilità al sindacato sull'esercizio del potere.

Non sempre, infatti, la pubblicazione in rete è garanzia di reale informazione, trasparenza e quindi "democraticità", perché comporta rischi di alterazione, manipolazione, decontestualizzazione e riproduzione per fini diversi, che potrebbero frustrare ogni esigenza di informazione veritiera e, quindi, di controllo, oltre che di oblio una volta venuta meno l'utilità del dato.

Di tali esigenze ci siamo fatti portatori rispetto al Governo, anche mediante un approfondimento congiunto con l'Anac, volto a individuare possibili linee di riforma.

La sfida reale è garantire dunque una trasparenza democratica e non demagogica, utile ai cittadini e non lesiva della loro persona.

Le sentenze on-line e la trasparenza della giustizia

Analoga sinergia tra privacy e trasparenza va garantita rispetto alle sentenze on-line. La pubblicazione sul web di dati preziosi, quali quelli ricavabili da una

sentenza e dai princìpi che vi sono affermati è, infatti, indubbiamente più "democratica", perché raggiunge, potenzialmente, tutti i cittadini, mettendo a disposizione un patrimonio informativo importante.

Ma questa facilità nell'accesso – straordinaria risorsa per i singoli e le istituzioni – è anche, paradossalmente, la più grande fonte di rischio delle pubblicazioni on-line, suscettibili di indicizzazione, riproduzione decontestualizzata, alterazione, e per questo in alcun modo assimilabili alle pubblicazioni cartacee.

Per questo, a legislazione vigente, abbiamo proposto la sottrazione delle sentenze dai motori di ricerca generalisti, così da coniugare il principio della pubblicità del processo – e del suo atto conclusivo – con la riservatezza dei soggetti a qualunque titolo coinvolti.

E dando, di una disciplina scritta 12 anni fa, un'interpretazione evolutiva, che tenga conto del quadro "costituzionale" europeo e delle differenze tra pubblicazione cartacea e telematica.

Si tratterebbe, oltretutto, di una soluzione analoga a quella utilizzata – anche su nostro impulso – proprio dalle Camere rispetto agli atti parlamentari, così da coniugare dignità individuale, pubblicità dei lavori e intangibilità degli atti parlamentari.

Ma oltre a deindicizzare le sentenze pubblicate integralmente, ci parrebbe più ragionevole favorire la massima conoscenza del patrimonio giuridico contenuto nelle sentenze, rendendole pubbliche il più possibile, ma oscurando i nomi presenti.

Si tratterebbe di una soluzione tanto più rilevante in un contesto, quale quello attuale, di progressiva telematizzazione del processo. In proposito, le garanzie suggerite nel tempo dal Garante al Governo, in sede di parere sui vari provvedimenti di disciplina del processo telematico, hanno consentito di fissare al punto più alto l'equilibrio tra trasparenza ed efficienza della giustizia da un lato e protezione dei dati personali, dall'altro.

Privacy, stampa e processi

Altrettanto importante per la qualità della nostra democrazia è il bilanciamento tra privacy e diritto all'informazione: tema su cui anche quest'anno non sono mancati interventi.

Importante, in particolare, la precisazione dei doveri di lealtà e correttezza cui il giornalista deve attenersi nell'esercizio della propria funzione, evitando soprattutto il ricorso ad artifici e raggiri o, perfino, come in un caso esaminato, alla sostituzione di persona.

Precisazione recentemente condivisa dall'Autorità giudiziaria in sede di impugnazione.

L'inchiesta giornalistica – che pure ha una funzione essenziale, da promuovere come straordinario strumento democratico – non può, infatti, ricorrere perfino a un atto che di per sé integra gli estremi di un reato, pur di carpire informazioni riservate e confidenziali.

Analogo esercizio di responsabilità è stato sollecitato in più occasioni, con riferimento alla cronaca giudiziaria e all'esigenza del rispetto del principio di essenzialità dell'informazione, infranto dalla divulgazione (spesso anche in violazione del regime di pubblicità degli atti investigativi sancito dal codice di rito) di ampi stralci o, addirittura, della versione integrale di atti d'indagine (interrogatori in carcere, intercettazioni), funzionali a soddisfare la curiosità del pubblico ma non reali esigenze informative rispetto al procedimento.

Il tutto con danno, spesso irreparabile, per i terzi – anche minori, talora vittime del reato – la cui esistenza viene in tal modo messa a nudo e riversata in rete, anche per sempre.

Abbiamo, quindi, adottato provvedimenti di blocco per impedire violazioni ulteriori in casi specifici di cronaca giudiziaria, sia riguardo ai terzi incolpevoli, sia rispetto a indagati di cui si è scandagliata sui giornali l'intera vita di relazione, senza alcuna connessione con le esigenze probatorie.

E abbiamo rappresentato al Governo la necessità di un riequilibrio nei

rapporti tra esigenze investigative, informazione e riservatezza, in un contesto di generale mediatizzazione della giustizia.

Il coinvolgimento a qualsiasi titolo in un procedimento non può, infatti, divenire la ragione, di per sé sufficiente, per esporre la parte o il terzo a una gogna che confonda il doveroso esercizio del diritto di cronaca con il sensazionalismo.

Auspichiamo pertanto che Parlamento e Governo vogliano farsi carico di quest'esigenza, coniugando gli aspetti della correttezza e lealtà dell'informazione e della riservatezza nelle indagini, nel rispetto del principio di proporzionalità tra privacy e mezzi investigativi ribadito, anche recentemente, dalla Corte di giustizia.

Diritto alla rete; diritti in rete

Quest'anno, in modo particolare, la rete è stata oggetto di un'attenzione crescente anche in sede parlamentare. Dalla Dichiarazione per i diritti in internet, ai disegni di legge costituzionale sull'accesso, alla disciplina del cyberbullismo e della tutela del minore, siamo stati partecipi di iniziative volte a sancire alcune minime garanzie per la dignità delle persone nell'Infosfera.

La rete costituisce una dimensione della vita entro cui si svolge – per citare l'art. 2 della Costituzione – la personalità di ciascuno.

Per questo e in questa misura, diviene un bene giuridico, meritevole di tutela soprattutto per non soccombere agli imperativi del mercato, per non rimettere a quella "legislazione privata" delle condizioni generali di contratto la garanzia, su scala mondiale, dei diritti fondamentali.

La sfida oggi, dunque, non è quella di giuridificare uno spazio che altrimenti, lasciato alla discrezionalità dell'etica individuale, troverebbe un suo ordine spontaneo: si tratta invece di difendere con determinazione la libertà di questo sterminato spazio pubblico.

Accanto alla straordinaria capacità di promuovere processi inclusivi, di partecipazione democratica e pluralistica, il web ha anche dimostrato – con

l'ambivalenza propria di ogni tecnologia – di poter amplificare, con effetti dirompenti, atti discriminatori, violenti, vessatori, spesso nei confronti dei soggetti più fragili o di quanti siano percepiti – e rappresentati – come diversi.

Dal *grooming* all'incitamento all'odio, alla violenza carnale – consumata off-line e poi esibita on-line, amplificandone così la potenza lesiva –; dalla "servitù volontaria" della prostituzione minorile, al cyberbullismo, nell'ampiezza delle sue accezioni.

Oltre al diritto alla rete, dunque, dobbiamo garantire, in rete, i diritti di tutti.

In primo luogo dei minori, vittime elettive di un uso distorto del web, perché non hanno gli strumenti per capire fino a che punto e con quali rischi esporre la propria vita, anche intima, agli altri.

La rete, paradossalmente, è il luogo in cui la fragilità dei minori emerge con maggior forza, in quello iato tra illusione di autonomia e introiezione di regole, esperienza della libertà ed esercizio di responsabilità.

La rete è anche il luogo in cui, nella presunzione di anonimato, minori violano altri minori.

E proprio questo è, forse, l'aspetto più tragico dell'uso violento della rete, in cui cioè l'autore e la vittima partecipano della stessa fragilità e della stessa inconsapevolezza del "risvolto" reale e concretissimo di ogni nostra azione nel digitale. Fenomeni che solo un esercizio consapevole del proprio diritto alla protezione dei dati personali e un nuovo codice etico della società digitale possono davvero contrastare.

È l'obiettivo che l'Autorità persegue ogni giorno, per far sì che la straordinaria "capacità generativa" della rete sia utilizzata non per violare, ma per promuovere i diritti di tutti.

L'Autorità: molti compiti, poche risorse

A fronte dei cambiamenti e degli scenari evocati, il Garante ha rafforzato e consolidato la propria attività.

Nel 2014 abbiamo adottato 628 provvedimenti collegiali, inclusi ricorsi e pareri resi al Governo. Sono 33.200 i quesiti ai quali l'Ufficio ha dato risposta, 577 sono state le sanzioni contestate, 385 le attività ispettive e di accertamento, svolte anche grazie all'ausilio della Guardia di Finanza, che unitamente al suo Comandante vogliamo ringraziare.

Un'attività intensa, anche a livello comunitario e internazionale, con la partecipazione ad oltre 80 riunioni, con importanti riconoscimenti per il lavoro svolto.

Siamo destinati a diventare parte integrante del sistema europeo dove il nuovo Regolamento ci affida compiti ancora più impegnativi e spinge verso modelli stringenti di collaborazione e condivisione con le altre Autorità.

Per questo, il ruolo del Garante deve essere rafforzato con mezzi e risorse adeguate, come richiesto dalla recente Conferenza di Manchester.

Ho rappresentato da tempo al Governo e al Parlamento l'urgenza di una seria revisione dell'attuale anacronistico sistema di finanziamento, non più sostenibile e tale da mettere fortemente a rischio, fino a precluderla del tutto, la nostra attività: in evidente contrasto con quanto imposto agli Stati membri dai Trattati.

Rinnoviamo la sollecitazione per una risposta non elusiva.

Prima di concludere, consentitemi di ringraziare le Colleghe Augusta Iannini, Licia Califano, Giovanna Bianchi Clerici che con me compongono il Collegio del Garante, con le quali condivido quotidianamente responsabilità e decisioni.

Desidero altresì ringraziare il Segretario generale Giuseppe Busia e coloro che nell'Ufficio, ogni giorno, lavorano con generosità e competenza per dare risposta alle crescenti domande di tutela dei cittadini.

In evidenza – 2014

Gennaio

A seguito di accertamenti avviati d'ufficio, abbiamo vietato l'uso dei dati personali riferiti a pazienti con insufficienza renale cronica da parte di un'associazione di medici nefrologi che gestisce un importante registro nazionale finalizzato allo svolgimento di analisi statistiche ed epidemiologiche (dati trasferiti anche in un analogo registro privato europeo), prescrivendo in pari tempo – al fine di soddisfare esigenze di ricerca medico-scientifica ritenute meritevoli – l'adozione di misure di sicurezza e di accorgimenti, ulteriori rispetto a quelli esistenti, volti ad assicurare l'anonimato degli interessati e ad informare gli stessi circa tale impiego ulteriore dei dati raccolti dalle strutture pubbliche di dialisi [par. 8.1]

Nel rispondere ad un quesito posto dalla Presidenza del Consiglio - Dipartimento per la funzione pubblica relativo alla legittimità di pubblicazione sul proprio sito web istituzionale dei nominativi dei fruitori di permessi sindacali, abbiamo affermato che, in base al d.lgs n. 33/2013 e al Codice, detti soggetti non rientrano tra coloro per i quali è prevista tale forma di pubblicità e che, al fine di soddisfare l'esigenza di trasparenza, è comunque possibile la pubblicazione in forma aggregata di tali informazioni [par. 13.3]

Abbiamo autorizzato un'azienda ospedaliero-universitaria a trattare i dati sanitari e genetici di circa duecento pazienti nell'ambito di uno studio monocentrico, approvato dal competente comitato etico, volto a monitorare gli esiti clinici di malati con cirrosi epatica sottoposti a trapianto di fegato nell'arco di cinque anni (con riguardo anche ai dati e ai campioni dei pazienti deceduti nel periodo successivo al trapianto, salvo che non si siano opposti in vita all'uso dei dati a scopo di ricerca), dopo aver informato e raccolto il consenso dei pazienti in vita [par. 7]

Parere favorevole è stato reso in merito allo schema di regolamento che definisce le modalità di funzionamento e collegamento della Banca nazionale unica della documentazione antimafia con il Ced interforze del Dipartimento della pubblica sicurezza ed altre banche dati. L'archivio, cui potranno accedere i soggetti che possiedono specifici profili di autorizzazione, consentirà di semplificare il sistema di rilascio della documentazione antimafia sulle imprese (cd. "comunicazioni" e "informazioni" antimafia) alle stazioni appaltanti e agli altri soggetti legittimati ad acquisirle (pubbliche amministrazioni, camere di commercio, ordini professionali ecc.) [parr. 9.2 e 3.4.1]

È stato reso un parere favorevole sullo schema di decreto del Ministero del lavoro relativo alla costituzione presso l'Inps del Casellario dell'assistenza, vale a dire l'anagrafe generale delle posizioni assistenziali, che ha accolto i suggerimenti forniti dall'Autorità (concernenti principalmente la selezione delle informazioni destinate a confluire nel casellario, l'individuazione dei soggetti che possono consultarle, le modalità di raccolta e di anonimizzazione dei dati relativi ai minori in situazioni di disagio) [parr. 4.2 e 3.4.1]

Febbraio

Alla luce delle mutate condizioni del mercato delle comunicazioni e della *number portability*, abbiamo aggiornato le prescrizioni impartite con il provvedimento generale del 25 giugno 2009 alle società telefoniche che svolgono attività di profilazione, permettendo l'analisi di alcune tipologie di dati della clientela in forma aggregata nell'intervallo temporale di due giorni [par. 12.4]

Visti gli esiti della consultazione pubblica, è stato adottato un provvedimento generale che impone agli operatori di *telemarketing* di adottare specifiche misure per ridurre drasticamente il fenomeno delle cd. "telefonate mute" [par. 12.2]

Marzo

È stata avviata una consultazione pubblica su uno schema di provvedimento relativo all'eventuale costituzione di una banca dati interoperatore dei clienti morosi nell'ambito dei servizi di comunicazione elettronica denominata Sit [par. 14.3]

Abbiamo dichiarato illecito e bloccato il trattamento dei dati effettuato da un ente pubblico mediante la diffusione sul proprio sito web istituzionale delle graduatorie (intermedia e definitiva) di un concorso riservato a disabili contenente dati idonei a rilevare lo stato di salute di oltre 500 concorrenti [par. 13.3]

Abbiamo fissato un quadro organico di regole per la tutela della riservatezza nel delicato ambito del trattamento dei dati da parte dei partiti politici in relazione agli aderenti e a quanti hanno contatti regolari nonché in relazione a simpatizzanti e partecipanti a singole iniziative (petizioni, proposte di legge, richieste di *referendum*). In un'ottica di semplificazione e contemperamento degli interessi, abbiamo esonerato in via definitiva partiti, movimenti, comitati e singoli candidati che fanno propaganda elettorale utilizzando alcune fonti pubbliche liberamente utilizzabili a tale scopo (ad es. le liste elettorali) dall'obbligo di rendere l'informativa dal sessantesimo giorno precedente la data delle consultazioni politiche, amministrative, referendarie o delle "primarie" al sessantesimo giorno successivo alla loro conclusione [par. 4.5]

Aprile

Su richiesta degli operatori di settore e considerati i mutamenti normativi e tecnologici, è stato promosso l'aggiornamento del codice di deontologia e buona condotta dei sistemi di informazione creditizia (sic) costituiti per verificare l'affidabilità, la puntualità nei pagamenti e il rischio di sovraindebitamento di quanti intendono accedere al credito al consumo [par. 14.2]

Abbiamo reso parere favorevole su uno schema di decreto del Presidente del Consiglio dei ministri in materia di destinazione del due per mille dell'irpef a favore di partiti politici, in base alla scelta del contribuente, evidenziando la necessità di una più puntuale definizione delle misure a tutela della riservatezza circa le determinazioni individuali, nonché, nella stessa materia, sullo schema di provvedimento del Direttore dell'Agenzia delle entrate con il quale è stata definita la scheda da utilizzare, in via transitoria, nell'esercizio finanziario 2014 per effettuare tale scelta [par. 2.1.1]

Abbiamo condizionato il parere favorevole reso su uno schema di regolamento del Ministero dell'Interno che individua le modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (Anpr) all'introduzione di una serie di misure ed accorgimenti, quali l'individuazione dei soggetti cui sono rimessi i controlli, il divieto di duplicazione delle anagrafi, la consultazione dell'Autorità sulla definizione di *standard* di qualità dei dati e l'adozione di elevate misure di sicurezza [parr. 4.5 e 3.4.1]

Maggio

Allo scopo di contemperare le esigenze di pubblicità e trasparenza con i diritti e le libertà fondamentali nonché la dignità delle persone, abbiamo individuato in apposite Linee guida cautele e misure da adottare quando sono diffusi sul web dati personali per finalità di trasparenza amministrativa in base al decreto legislativo n. 33/2013. Si è inoltre chiarito che i dati così pubblicati non sono liberamente utilizzabili da chiunque per qualunque finalità, ma solo in termini compatibili con gli scopi per i quali sono raccolti [par. 4.4]

Con provvedimento di carattere generale, abbiamo individuato modalità semplificate per rendere l'informativa *online* sui trattamenti effettuati mediante *cookie*: all'utente deve essere chiaramente ed immediatamen-

te rappresentato se il sito utilizza *cookie* di profilazione per inviare messaggi pubblicitari mirati o se il sito consente anche l'invio di *cookie* di "terze parti" (ossia di *cookie* installati da un sito diverso tramite il sito che si sta visitando). Deve essere assicurato un *link* a un'informativa più ampia sull'utilizzo dei *cookie* e la possibilità di negare il consenso alla loro installazione [par. 11.5]

Anche tenendo conto delle indicazioni pervenute in sede di consultazione pubblica, abbiamo impartito prescrizioni ai titolari che effettuano trattamenti dati in ambito *mobile payment* utilizzando *smartphone*, *tablet* e pc [par. 12.6]

A seguito dello *Sweep Day* dedicato al controllo di *app* per *smartphone* e *tablet*, le Autorità che hanno partecipato all'iniziativa, e tra queste il Garante, hanno reso pubblica la lettera congiunta indirizzata alle maggiori piattaforme e agli operatori del mercato delle *app*, evidenziando i numerosi casi di *app* prive di qualsiasi *privacy policy* [par. 23.5]

È stato espresso parere favorevole su uno schema di decreto del Presidente del Consiglio dei ministri che consentirà a Regioni e Province autonome di dare il via al fascicolo sanitario elettronico (Fse) con il quale si individuano i primi contenuti da attivare a livello nazionale (l'informativa da rendere ai pazienti; i dati e i documenti da inserire, con opzioni rimesse alla volontà individuale; le responsabilità e i compiti dei soggetti coinvolti; le garanzie e le misure di sicurezza da adottare nel trattamento dei dati personali; le modalità e i livelli diversificati di accesso al fascicolo; i criteri di interoperabilità nonché i contenuti informativi e le codifiche del profilo sanitario sintetico e del referto di laboratorio) [parr. 6.1.2 e 3.4.1]

Abbiamo dato notizia al Presidente del Consiglio dei ministri delle rilevanti criticità emerse nel corso di una serie di ispezioni presso gli *Internet eXchange Point* (Ixp) nazionali – presso i quali si interconnettono le infrastrutture di rete dei maggiori operatori di tlc nazionali e internazionali, degli *Internet service provider*, nonché di importanti fornitori di servizi *online* e che, tra l'altro, ospitano gli apparati che gestiscono le reti di comunicazione tra quasi tutte le pubbliche amministrazioni italiane nonché quelle degli enti di ricerca – al fine di consentirne la tempestiva valutazione da parte degli organismi preposti alla sicurezza cibernetica del Paese [par. 22.3]

Abbiamo accolto la richiesta di verifica preliminare presentata dalla Banca d'Italia relativa all'uso di sistemi di videosorveglianza "intelligente" in relazione agli specifici rischi connessi allo stoccaggio e alla gestione di elevate quantità di valori [par. 4.8]

Giugno

Abbiamo reso il parere su uno schema di decreto del Presidente del Consiglio dei ministri recante la definizione delle caratteristiche del Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (Spid) – Sistema volto, nel suo complesso, a favorire la diffusione di servizi in rete mediante l'attribuzione a ciascun soggetto interessato di un'"identità digitale" – nonché dei tempi e delle modalità di sua adozione da parte di pubbliche amministrazioni e imprese [parr. 4.2 e 3.4.1]

È stato aggiornato il codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale (All. A3 al Codice) [par. 8.2]

Luglio

Dopo aver seguito fin dall'inizio (2012) il negoziato in seno al Gruppo di lavoro del Consiglio UE (DAPIX) incaricato di licenziare le modifiche alle proposte di Regolamento e di Direttiva in materia di protezione dei dati personali, abbiamo rafforzato la collaborazione con il Governo in occasione del

semestre di Presidenza italiana dell'UE nel corso del quale si è raggiunto un accordo fra gli Stati Membri su punti essenziali della Proposta di Regolamento (trasferimento di dati verso Paesi terzi, obblighi di responsabili e incaricati del trattamento, trattamenti per finalità di pubblico interesse) e si è fatta maggiore chiarezza sul campo di applicazione della Proposta di Direttiva concernente le attività giudiziarie e di polizia [par. 23.1]

Abbiamo disposto il blocco rispetto alla diffusione da parte di alcune testate delle trascrizioni delle intercettazioni telefoniche riguardanti la vicenda di un fotografo accusato di reati sessuali nei confronti di minorenni, non rispettosa dei limiti del diritto di cronaca e dell'essenzialità dell'informazione [par. 10.1]

Abbiamo prescritto a Google di adottare un'informativa per gli utenti strutturata su più livelli e di acquisire il previo consenso degli stessi – ancorché con modalità semplificate – in caso di utilizzo dei dati a fini di profilazione e pubblicità comportamentale personalizzata; dovranno essere altresì definiti tempi certi di conservazione dei dati (conservati sui sistemi cd. "attivi" ovvero di *back up*) [par. 11.2]

Abbiamo negato l'autorizzazione all'installazione di un sistema di videosorveglianza all'interno degli spogliatoi dei dipendenti considerate le caratteristiche invasive dello stesso su riservatezza e dignità degli interessati (nonché considerata la sua scarsa utilità nel contrasto di furti comunque avvenuti in altri locali aziendali) [par. 13.1]

Anche alla luce delle Linee guida del Garante del 2009, in più occasioni siamo intervenuti presso aziende sanitarie e strutture ospedaliere per assicurare la correttezza nelle fasi di realizzazione e successivo utilizzo dei *dossier* sanitari elettronici, prescrivendo misure per la tenuta dei dati personali, e idonei accorgimenti, anche tecnici, per selezionare l'accesso agli stessi nonché per consentire all'interessato di ottenere l'oscuramento di singoli eventi clinici [par. 6.1.2]

Abbiamo reso parere favorevole sul sistema di ripresa delle immagini avviato in via sperimentale dal Dipartimento della pubblica sicurezza in quattro città mediante microtelecamere indossabili dagli agenti di polizia nel corso di manifestazioni pubbliche ed attivabili solo in caso di criticità, con l'indicazione di misure sulla tenuta delle schede video nonché su modalità e tempi di conservazione dei dati registrati [par. 9.2]

Abbiamo reso un parere favorevole sulle modifiche apportate dal Coni al proprio regolamento per il trattamento dei dati sensibili e giudiziari, con particolare riferimento ai trattamenti di dati che riguardano un gruppo selezionato di atleti (inseriti nel *registered testing pool* nazionale) effettuati attraverso l'*Anti-Doping Administration & Management System* (ADAMS), rispetto ai quali il Coni potrà effettuare, ove necessario, operazioni di trasferimento all'estero, verso la banca dati ADAMS e verso le organizzazioni *anti-doping* ubicate anche in Paesi terzi di volta in volta competenti a testare gli atleti [par. 4.1]

Abbiamo reso parere favorevole – con riserve rispetto al previsto scambio di dati sul dna verso Paesi terzi – sullo schema di regolamento, attuativo della legge 30 giugno 2009, n. 85, in materia di banca dati nazionale del dna e laboratorio centrale per la banca dati nazionale del dna [parr. 9.2 e 3.4.1]

Settembre

Abbiamo ritenuto illecita l'acquisizione e la diffusione radiofonica della registrazione del contenuto di una comunicazione telefonica intercorsa con un esponente politico ed effettuata da parte di un giornalista utilizzando, in violazione del principio di correttezza, un "artificio" (segnatamente, l'imitazione della voce di un altro esponente politico amico dell'interessato) [par. 10.3]

Abbiamo ritenuto ammissibile il trattamento di dati personali effettuato attraverso la localizzazione di dispositivi *smartphone* forniti ai dipendenti per finalità organizzative e di sicurezza sul lavoro, nel rispetto dell'art. 4 dello Statuto dei lavoratori, purché non vengano trattati altri dati (sms, telefonate) e siano adottate opportune misure di sicurezza [par. 13.1]

Ottobre

Abbiamo vietato ad una società di intermediazione di prestiti *online* l'utilizzo dei dati personali degli utenti forniti nella richiesta di preventivo per la diversa finalità di *marketing* in assenza di un consenso liberamente prestato a tal fine [par. 11.3]

A seguito di consultazione pubblica, abbiamo adottato un provvedimento generale (con le allegate Linee guida) in materia di dati biometrici grazie al quale, nel rispetto del principio di minimizzazione e con l'individuazione di numerose misure di sicurezza, sono state identificate alcune tipologie di trattamento che, per le finalità perseguite, presentano un livello ridotto di rischio e non necessitano della verifica preliminare da parte dell'Autorità, in particolare in relazione a forme di autenticazione informatica, per il controllo di accesso fisico ad aree "sensibili" (ad es. destinate all'utilizzo di apparati e macchinari pericolosi), per la sottoscrizione di documenti informatici nonché per scopi cd. facilitativi [par. 15.2]

Novembre

Abbiamo stabilito che le strutture sanitarie non possano raccogliere in maniera sistematica e preventiva informazioni sulle convinzioni religiose dei pazienti e, più in generale, quando ciò non sia indispensabile [par. 6.1]

Abbiamo adottato i primi provvedimenti dopo la sentenza della Corte di giustizia nel caso "Google Spain" relativi alle richieste di cancellazione dai risultati dei motori di ricerca in Internet dei collegamenti alle pagine web che contengono il nominativo dell'interessato [par. 10.4]

Abbiamo reso parere favorevole su uno schema di provvedimento del Ministero del lavoro concernente il modello di Dichiarazione sostitutiva unica (Dsu) necessario per il calcolo dell'Isee, lo strumento di valutazione della situazione economica di coloro che richiedono prestazioni sociali agevolate. Gli interessati dovranno essere informati in modo chiaro sull'uso che viene fatto dei loro dati (finalità, tempi di conservazione, ambito di comunicazione) mediante apposita informativa inserita nella parte iniziale della dichiarazione (dalla quale dovrà altresì risultare che i controlli dell'Inps sulle informazioni fornite dal dichiarante si estenderanno anche a dati personali dei componenti il nucleo familiare, quali la situazione reddituale e patrimoniale) [parr. 4.2 e 3.4.1]

Dicembre

Abbiamo rinnovato le autorizzazioni generali per il trattamento di dati sensibili e giudiziari [par. 1]

Nel parere reso all'Istituto nazionale della previdenza sociale (Inps) avente ad oggetto uno schema di convenzione tra l'Istituto e Confindustria, Cgil, Cisl e Uil (prevista dal "Testo unico sulla rappresentanza" sottoscritta il 10 gennaio 2014), abbiamo evidenziato che per misurare la rappresentatività sindacale nel settore privato ai fini della contrattazione nazionale di categoria non è necessaria la trasmissione da parte delle imprese all'Inps dei dati concernenti l'affiliazione sindacale di ciascun lavoratore, potendosi perseguire lo stesso fine mediante la sola rilevazione del numero di deleghe assegnate a ciascuna sigla sindacale [par. 13]

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

1 Introduzione: i principali interventi dell'Autorità nel 2014

1.1. Se la materia della protezione dei dati personali trascende i confini nazionali (e fin dalle origini aspira ad estendersi su scala globale), non pare revocabile in dubbio che nel 2014 questa vocazione naturale si sia pienamente manifestata, sia in relazione ai passi avanti fatti nell'opera di ammodernamento del quadro normativo di riferimento (nell'ambito dell'Unione europea come pure del Consiglio d'Europa), sia per la significatività (e gli effetti) delle sentenze pronunciate dalla Corte di giustizia dell'Unione europea.

Entrambi gli sviluppi cui si è appena fatto cenno non sono rimasti senza effetti sull'attività dell'Autorità, che da sempre si caratterizza per dinamismo nell'ambito del Gruppo dei Garanti europei istituito dall'art. 29 della direttiva 95/46/CE – del quale, a novembre, il Presidente dell'Autorità è stato eletto vicepresidente – e sui diversi tavoli internazionali nei quali è chiamata ad operare (cfr. par. 23 e, per un quadro di sintesi, i dati riepilogativi riportati nella sez. IV, tab. 25).

Dopo aver seguito fin dalle prime battute il negoziato in seno al Gruppo di lavoro del Consiglio UE (DAPIX), nell'ambito del processo legislativo che dovrebbe portare all'adozione delle Proposte di Regolamento e di Direttiva in materia di protezione dei dati personali, l'Autorità ha rafforzato la collaborazione con il Governo in occasione del semestre di Presidenza italiana dell'UE, arco temporale nel corso del quale si è raggiunto un accordo fra gli Stati membri su alcuni elementi essenziali della Proposta di Regolamento (trasferimento di dati verso Paesi terzi, obblighi di titolari e responsabili del trattamento, trattamenti per finalità di pubblico interesse) e si è fatta maggiore chiarezza sul campo di applicazione della Proposta di Direttiva concernente le attività giudiziarie e di polizia (par. 23.1).

L'Autorità ha operato attivamente anche nell'ambito del Comitato intergovernativo incaricato dal Comitato dei ministri di portare a termine il processo di modernizzazione della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale n. 108/1981 del Consiglio d'Europa, conclusosi con l'adozione, nel dicembre 2014, del documento contenente la Convenzione modernizzata che attende ora la definitiva approvazione del Comitato dei ministri (par. 23.5).

1.2. Si è già fatto cenno alle sentenze pronunciate dalla Corte di giustizia, i cui assunti potranno riverberare nella più ampia discussione del *legal framework* europeo,

ma i cui effetti già in parte si registrano nell'ordinamento nazionale: ciò vale per la definizione dell'(ampio) ambito di applicazione della direttiva 95/46/CE (e quindi delle discipline nazionali di recepimento), sia con riguardo all'utilizzo di sistemi di videosorveglianza per finalità personali – quando in grado di riprendere aree pubbliche ancorché posti a presidio del domicilio da parte di privati (11 dicembre 2014, František Ryneš c. Úřad pro ochranu osobních údajů, causa C-212/13: par. 14.5) –, sia in relazione a soggetti stabiliti in Paesi terzi, segnatamente Google, società ritenuta titolare del trattamento concernente i dati personali pubblicati *online* da terzi e rinvenibili utilizzando le funzionalità del motore di ricerca (13 maggio 2014, C-131-12, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos e Mario Costeja González: cfr. par. 10.4).

Invece, non solo è rimasta senza effetti nell'ordinamento nazionale – segnatamente rispetto alla disciplina contenuta nell'art. 132 del Codice – la sentenza (già segnalata nella Relazione 2013) dell'8 aprile 2014 (Digital Rights Ireland e Seitlinger e a., cause riunite C-293/12 e C-594/12), con la quale la Corte di giustizia ha dichiarato invalida la direttiva sulla conservazione dei dati di traffico, ritenendo che dalla stessa derivi un'ingerenza di ampia portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati, ma anzi il Garante ha dovuto nuovamente richiamarne i contenuti in occasione delle misure (ulteriormente invasive) introdotte in sede di conversione del decreto-legge 18 febbraio 2015, n. 7, la cui portata, in particolare all'art. 4-*bis*, è stata solo in parte attenuata nel testo definitivo della legge di conversione 17 aprile 2015, n. 43 (cfr. doc. web n. 3807700).

Non può trascurarsi, infine, la circostanza che la Corte sia tornata a pronunciarsi, per la terza volta, sul tema dell'indipendenza delle autorità di protezione dei dati personali (8 aprile 2014, Commissione c. Ungheria, causa C-288/12), carattere irrinunciabile nell'architettura costituzionale europea risultante dal disegno tracciato dalla Carta dei diritti fondamentali dell'Unione europea (art. 8) e dai Trattati (artt. 16 TFUE e 39 TUE).

1.3. Ma l'impegno dell'Autorità, pur catalizzato dal processo di cambiamento in essere presso le Istituzioni sovranazionali in ragione delle sue ricadute sull'ordinamento interno, non si è limitato a (e tanto meno esaurito in) quanto accade oltreconfine (per uno sguardo d'insieme, v. i dati statistici riportati nella sez. IV, tab. 1). Costante e fattivo è infatti il rapporto collaborativo consolidatosi negli anni con il Governo e le singole Amministrazioni del quale sono visibili i frutti, anzitutto nei pareri resi (scanditi nel par. 3.4), in relazione ai quali, diversamente da quanto accaduto negli anni precedenti, non si sono registrati casi di mancata consultazione del Garante. Dall'esame del loro contenuto si desume che il Garante è chiamato a pronunciarsi (a volte con una tempistica serrata) nelle materie più disparate, sempre più spesso soffermandosi anche su complessi profili tecnologici.

Gli ambiti toccati riguardano i principali progetti di modernizzazione del Paese – quali il Sistema pubblico per la gestione dell'identità digitale di cittadini ed imprese (Spid) (par. 4.2) o l'Anagrafe nazionale della popolazione residente (Anpr) (par. 4.5) –, i sistemi informativi preordinati ad incrementare l'efficienza dell'azione amministrativa – si pensi al Casellario dell'assistenza (par. 4.2), al Sistema informativo nazionale per la prevenzione nei luoghi di lavoro (Sinp) (par. 4.2) o alla Banca nazionale unica della documentazione antimafia (par. 9.2) – e, ancora, gli archivi orientati ad un più efficace contrasto ai fenomeni criminali nel rispetto dei diritti fondamentali degli interessati, come nel caso della progettata banca dati nazionale del dna (par. 9.2).

Attenzione è stata anche posta, in attesa del completamento del faticoso processo che dovrebbe condurre all'adozione della direttiva per i trattamenti effettuati per

finalità di polizia e giustizia, ai delicati trattamenti effettuati in via sperimentale dal Dipartimento della pubblica sicurezza in quattro città mediante micro-telecamere indossate dagli agenti di polizia nel corso di manifestazioni pubbliche ed attivabili solo in caso di criticità, con l'indicazione di misure sulla tenuta delle schede video nonché su modalità e tempi di conservazione dei dati registrati (par. 9.2). Ma pure il Garante è stato chiamato a rendere il proprio parere, nel quale si sono evidenziate criticità, su uno schema di regolamento, attuativo della legge 30 giugno 2009, n. 85, in materia di banca dati nazionale del dna e sul laboratorio centrale per la banca dati nazionale del dna (par. 9.2).

La cooperazione istituzionale si è altresì manifestata nelle segnalazioni indirizzate a Parlamento e Governo una volta ravvisata dal Garante la necessità di interventi normativi innovativi o correttivi (par. 3.1) – come accaduto in relazione alle proposte caldeggiate dall'Autorità per una revisione dell'apparato sanzionatorio del Codice e per l'attualizzazione delle (ormai superate) misure minime di sicurezza (par. 22.7) o, ancora, con riguardo alla materia, delicatissima, dell'accesso ai dati concernenti le proprie origini biologiche, a seguito della nota sentenza della Corte costituzionale n. 278/2013 (par. 6.1.4). Nella stessa prospettiva si collocano i contributi presentati dall'Autorità alla luce dei temi in discussione in sede parlamentare, anzitutto in sede di audizione (par. 3.2) e con riguardo agli atti di sindacato ispettivo concernenti le materie di proprio interesse (par. 3.3), come pure con la partecipazione alle iniziative che hanno fatto corona alla proposta formulata dalla Commissione di studio per l'elaborazione di principi in tema di diritti e doveri relativi ad internet, istituita dalla Presidente della Camera dei deputati, formulando opinioni a margine della stessa: dapprima nell'ambito del Convegno "Verso una Costituzione per Internet?", quindi, nel corso di un'audizione tenutasi il 12 gennaio 2015, con l'intervento del presidente Soro, unitamente ai Presidenti dell'Autorità garante della concorrenza e del mercato e dell'Autorità garante per le comunicazioni (par. 24.6).

1.4. Che il mondo di internet appena evocato rientri tra le priorità dell'Autorità, con particolare riguardo alle tematiche che interessano i minori, emerge peraltro con chiarezza già dal tema scelto per celebrare la Giornata europea della protezione dei dati personali 2014, "Educare alla rete. L'alfabeto della nuova cittadinanza nella società digitale", come pure dai diversi provvedimenti adottati in questa materia: da quello che individua modalità semplificate per rendere l'informativa *online* sui trattamenti effettuati mediante *cookies* (in particolare per finalità di profilazione e *marketing*) (par. 11.5), ai provvedimenti che il Garante (non diversamente da altre autorità) ha adottato dopo la menzionata sentenza della Corte di giustizia nel caso "Google Spain" relativi alle richieste di cancellazione dai risultati dei motori di ricerca in internet dei collegamenti alle pagine web che contengono il nominativo dell'interessato (par. 10.4); e, ancora, in quest'ambito vanno considerati i provvedimenti (inibitori e prescrittivi) relativi all'indebito utilizzo (in assenza il consenso degli interessati) dei dati personali forniti per conseguire preventivi *online* per l'accesso al credito, successivamente trattati per finalità promozionali (par. 11.3).

E se, sempre nel contesto della rete, l'Autorità incontra talvolta difficoltà nell'acquisizione di sicuri elementi di valutazione nella propria attività di controllo (anche d'ufficio) (cfr. par. 11.4) – ad esempio, rispetto alla pratica (purtroppo sempre attuale) dello *spam* (par. 12.7) –, è pur vero che si vanno (utilmente) sperimentando forme di cooperazione con altre autorità di protezione dei dati personali, dando corpo a quanto da tempo discusso e messo a punto negli incontri e nelle conferenze internazionali tra Garanti (parr. 23.2 e 23.4). In questa cornice deve essere inserita l'attività connessa allo *Sweep Day* dedicato al controllo di *app* mediche per *smartphone* e *tablet*, all'esito

del quale le Autorità che vi hanno preso parte, e tra queste il Garante, hanno reso pubblica la lettera congiunta indirizzata alle maggiori piattaforme e agli operatori del settore, evidenziando i numerosi casi di *app* prive di qualsiasi *privacy policy* (par. 23.5). Nel medesimo ambito vanno pure annoverate le iniziative condotte nei confronti di Google, rispetto alle quali il Garante ha adottato un provvedimento che richiede, anzitutto, maggiore trasparenza nei confronti degli utenti, prescrivendo alla società, che (tra l'altro) gestisce il diffusissimo motore di ricerca, di adottare un'informativa strutturata su più livelli, nonché di acquisire il previo consenso degli interessati – ancorché con modalità semplificate – in caso di utilizzo dei dati a fini di profilazione e pubblicità comportamentale personalizzata (par. 11.2).

1.5. Le iniziative di *spending review* che hanno continuato ad interessare l'Autorità – concretizzatesi non solo nella razionalizzazione nell'impiego delle risorse disponibili (parr. 25.2 e 25.3), ma anche nella rinuncia alla disponibilità della Sala conferenze e al significativo ridimensionamento della Biblioteca, "luoghi" elettivi di incontro, studio e comunicazione qualificata con la comunità (parr. 24.8 e 24.9) – nonché le preoccupazioni connesse alla continuità nel finanziamento dell'attività istituzionale (rinfocolate dagli effetti riflessi di recenti pronunce del Giudice amministrativo) (par. 25.1), non hanno impedito al Garante di continuare ad assolvere – peraltro con un significativo incremento nelle somme incassate per le sanzioni contestate (cfr. par. 22.5 e sez. IV, tab. 1 e 8) – i propri compiti istituzionali. Quello di sentinella della società italiana a fronte delle possibili derive tecnologiche, mediante una rinnovata e multiforme attività di comunicazione (cfr. par. 24 e sez. IV, tab. 2), ma pure di organo cui è rimesso il controllo sulla liceità dei trattamenti di dati personali effettuati nel Paese (par. 22). Al riguardo, in presenza di una domanda sociale che, nel suo complesso, non è venuta meno negli anni (ed anzi va acuendosi in taluni settori) (cfr. sez. IV, tab. 9 e 10), si segnalano qui solo alcuni degli interventi maturati nel corso del 2014 – sovente frutto delle attività ispettive *in loco* effettuate dal personale dell'Autorità (sempre più spesso associando competenze tecniche e giuridiche) o, sulla base di un protocollo d'intesa ormai sperimentato, con il prezioso contributo della Guardia di finanza, in particolare tramite il Nucleo speciale *privacy* (parr. 22.2 e 22.4) –, la cui analisi trova compiuto svolgimento nel corpo della Relazione.

1.6. Inalterata è stata l'attenzione dell'Autorità nei confronti dei trattamenti che possono incidere in profondità sui diritti delle persone, quali quelli effettuati con dati sensibili e giudiziari, rispetto ai quali il Garante ha rinnovato l'11 dicembre 2014 le autorizzazioni generali al trattamento (pubblicate in *G.U.* 30 dicembre 2014, n. 301). Entro questa cornice, significativi sono i provvedimenti volti a promuovere la dignità della persona all'interno delle strutture sanitarie – precludendo la raccolta sistematica e preventiva di informazioni sulle convinzioni religiose dei pazienti quando ciò non sia indispensabile (par. 6.1) – ed incentrati sul trattamento di dati relativi alle condizioni di salute. A quest'ultimo riguardo, anzitutto nel contesto più strettamente sanitario, coerentemente con gli interventi già svolti in passato (cfr. Relazione 2013, p. 15 s.), è stato espresso parere favorevole su uno schema di decreto del Presidente del Consiglio dei ministri che, individuando i primi contenuti da attivare a livello nazionale, consentirà a Regioni e Province autonome di dare il via al Fascicolo sanitario elettronico (Fse) (par. 6.1.2); inoltre, verifiche sono state effettuate circa il corretto impiego dei *dossier* sanitari all'interno delle strutture di cura (par. 5.1.2).

Per quanto attiene, invece, all'utilizzo di dati sanitari (e genetici) al di fuori del contesto strettamente terapeutico – anzitutto per finalità di ricerca medico-scientifica –, il Garante è stato chiamato ad intervenire, con divieti e prescrizioni, in rela-

zione all'uso dei dati riferiti a soggetti affetti da insufficienza renale cronica veicolati (senza le dovute garanzie) in un importante registro nazionale (e quindi europeo) finalizzato allo svolgimento di analisi statistiche ed epidemiologiche (par. 8.1), ma pure ha autorizzato un'azienda ospedaliero-universitaria a trattare i dati sanitari e genetici di circa duecento malati nell'ambito di uno studio monocentrico, approvato dal competente comitato etico, volto a monitorare gli esiti clinici di pazienti con cirrosi epatica (ancora in vita e defunti) sottoposti a trapianto di fegato (par. 7).

1.7. Sotto la pressione delle istanze che pervengono all'Autorità, il trattamento dei dati personali nel contesto lavorativo si segnala ancora come uno degli ambiti elettivi di intervento del Garante: per porre un argine a gravi violazioni della dignità dei lavoratori – come nel caso che ha determinato il diniego opposto dal Garante all'autorizzazione di trattamenti di immagini rilevate da sistemi di videosorveglianza da installare in spogliatoi aziendali (par. 13.1) – ma pure per ammettere, per finalità organizzative e di sicurezza sul lavoro, il trattamento di dati personali effettuato attraverso la localizzazione di dispositivi *smartphone* forniti ai dipendenti nel rispetto della disciplina sui controlli a distanza contenuta nello Statuto dei lavoratori (par. 13.1). Disciplina, quest'ultima, che potrà essere rivisitata, in base a quanto previsto dall'art. 1, comma 7, lett. *f*), l. 10 dicembre 2014, n. 183, alla luce "dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore" e, in questa prospettiva, tenendo opportunamente conto della recente Raccomandazione adottata il 1° aprile scorso dal Consiglio dei ministri del Consiglio d'Europa CM/Rec(2015)5 sul trattamento dei dai personali in ambito lavorativo.

1.8. Allo scopo di contemperare le legittime esigenze di pubblicità e trasparenza amministrativa con i diritti e le libertà fondamentali nonché la dignità delle persone – tema ormai da tempo nell'agenda del Garante e sul quale si sono registrati anche nel 2014 interventi puntuali, come nel caso del blocco della diffusione effettuata da un ente pubblico mediante il proprio sito web delle graduatorie di un concorso riservato a disabili contenente dati idonei a rilevare lo stato di salute di oltre 500 concorrenti (par. 13.3) –, sono state individuate, in apposite Linee guida, cautele e misure da adottare quando sono diffusi sul web dati personali per finalità di trasparenza in base al decreto legislativo n. 33/2013; si è inoltre chiarito che i dati così pubblicati non sono liberamente utilizzabili da chiunque per qualunque finalità, ma solo in termini compatibili con gli scopi per i quali sono raccolti (parr. 4.4 e 13.3).

Nella stessa materia, nel rispondere ad un quesito posto dal Ministero per la funzione pubblica relativo alla legittimità della pubblicazione sul sito web istituzionale dei nominativi dei fruitori di permessi sindacali, il Garante ha affermato che, in base al d.lgs n. 33/2013 e al Codice, tali soggetti non rientrano tra coloro per i quali è prevista detta forma di pubblicità e che, al fine di soddisfare l'esigenza di trasparenza, è comunque possibile la pubblicazione in forma aggregata di dette informazioni (par. 13.3).

1.9. Ma, al di là dello svolgimento dei compiti di controllo ai quali si è fatto sinteticamente richiamo, il Garante continua ad essere autorità "dialogante", oltre che con la società nel suo complesso, in particolare con le categorie rappresentative di settori nei quali il corretto trattamento dei dati personali può essere co-regolato mediante il peculiare strumento dei codici di deontologia e di buona condotta previsti dall'art. 12 del Codice. Ancorché non sia stato purtroppo possibile concludere i lavori, avviati su iniziativa del Garante, volti ad aggiornare il codice di condotta dei

giornalisti (come anticipato nella Relazione 2013, p. 86), è stato invece premiato lo sforzo fatto per attualizzare il codice di deontologia per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale (par. 8.2).

A ciò va aggiunto che, su richiesta degli operatori di settore (considerati i mutamenti normativi e tecnologici), è stato altresì promosso l'aggiornamento del codice di deontologia dei sistemi di informazione creditizia (sic), risalente al 2004 e per il quale, con sguardo retrospettivo, può certamente formularsi un bilancio positivo (par. 14.2).

I lavori da tempo avviati per la redazione del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale hanno portato inoltre all'adozione di una bozza di codice sottoposta a consultazione pubblica nel febbraio 2015 (doc. web n. 3777733).

Può infine rilevarsi che lo strumento della consultazione pubblica si è rivelato prezioso anche per l'adozione di importanti provvedimenti di natura generale: si pensi a quelli concernenti la materia del trattamento dei dati biometrici, con l'individuazione di ambiti significativi per il quali si sono introdotte semplificazioni (par. 15.2), come pure in relazione ai trattamenti di dati effettuati, utilizzando *smartphone*, *tablet* e pc, in ambito *mobile payment* (par. 12.6); ovvero a quello adottato per porre un argine al fenomeno delle cd. "telefonate mute" da parte degli operatori di *telemarketing* (par. 12.2) e, ancora, a quello con cui si sono aggiornate le prescrizioni dirette ai fornitori di servizi di comunicazione elettronica accessibili al pubblico in punto di profilazione (par. 12.4). Sotto diverso profilo, lo stesso strumento della consultazione ha reso evidenti le posizioni contrapposte dei portatori dei diversi interessi in gioco rispetto ad uno schema di provvedimento relativo all'eventuale costituzione di una banca dati interoperatore dei clienti morosi nell'ambito dei servizi di comunicazione elettronica (denominata Sit), con la conseguente decisione dell'Autorità di avviare un'ulteriore fase di confronto diretto tra le parti, tuttora in corso, al fine di pervenire, se possibile, ad una decisione in grado di contemperare le contrapposte esigenze (par. 14.3).

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

Nel corso del 2014 sono stati approvati numerosi provvedimenti normativi con riflessi in materia di protezione dei dati personali. Fra questi, al fine di offrirne una (seppur sintetica) ricognizione, tale però da rendere conto dell'ampiezza e dell'eterogeneità delle materie che rientrano nell'area di interesse dell'Autorità, si ricordano:

Legge di stabilità 2015

1) la legge 23 dicembre 2014, n. 190, recante disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge di stabilità 2015), nella parte in cui istituisce il Registro nazionale dei donatori di cellule riproduttive a scopi di procreazione medicalmente assistita di tipo eterologo (art. 1, comma 298). Il Registro è istituito presso l'Istituto superiore di sanità, Centro nazionale trapianti e nell'ambito del Sistema informativo trapianti (Sit) di cui alla legge 10 aprile 1999, n. 91, al fine di garantire, in relazione alle tecniche di procreazione medicalmente assistita di tipo eterologo, la tracciabilità del percorso delle cellule riproduttive dal donatore al nato e viceversa nonché il conteggio dei nati generati dalle cellule riproduttive di un medesimo donatore. Nel Registro sono presenti tutti i soggetti ammessi alla donazione mediante l'attribuzione ad ogni donatore di un codice. A tal fine, le strutture sanitarie autorizzate al prelievo e al trattamento delle cellule riproduttive comunicano al Registro i dati anagrafici dei donatori, con modalità informatiche predefinite, idonee ad assicurare l'anonimato dei donatori medesimi. Fino alla completa operatività del Registro, i predetti dati sono comunicati al Centro nazionale trapianti con modalità cartacea, salvaguardando comunque l'anonimato dei donatori. La materia è di estrema delicatezza e richiede disposizioni normative e procedure di attuazione conformi ai principi e alle regole in materia di protezione dei dati personali, con il doveroso coinvolgimento del Garante al fine di individuare le misure necessarie per assicurare il rispetto del diritto alla protezione dei dati personali.

***Jobs Act* e controllo a distanza**

2) la legge 10 dicembre 2014, n. 183, recante deleghe al Governo in materia di lavoro, con particolare riferimento al previsto decreto legislativo per la redazione di un testo organico semplificato delle discipline dei contratti e dei rapporti di lavoro. Fra i criteri direttivi cui deve attenersi il decreto vi è, infatti "la revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro" da realizzare tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive e organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore (art. 1, comma 7, lett. *f*). Il tema è di notevole interesse per le evidenti implicazioni sulla disciplina in materia di protezione dei dati personali nel rapporto di lavoro (art. 114 del Codice; art. 4, l. n. 300/1970) ed in relazione al quale, al di là dei numerosi provvedimenti adottati nel tempo relativi a fattispecie individuali, proprio per tener conto dell'evoluzione tecnologica, il Garante ha formulato, con la delibera 1° marzo 2007, n. 13, apposite Linee guida dedicate ai trattamenti di dati personali effettuati in relazione all'impiego sul luogo di lavoro della posta elettronica nonché concernenti la "navigazione" in internet (doc. web n. 1387522);

Accordo Italia-USA e contrasto a criminalità

3) la legge 3 luglio 2014, n. 99, di ratifica ed esecuzione dell'Accordo fra la Repubblica italiana e gli Stati Uniti d'America sul rafforzamento della cooperazione nella prevenzione e lotta alle forme gravi di criminalità, fatto a Roma il 28 maggio 2009. L'art. 2, comma 2, della legge prevede che, al fine di assicurare la migliore operatività dell'Accordo, entro 150 giorni dalla sua entrata in vigore, siano adottati i decreti previsti dagli artt. 46, 49, 53 e 57 del Codice. Si tratta dei provvedimenti con cui il Ministero della giustizia e il Ministero dell'interno devono individuare i trattamenti di dati effettuati, rispettivamente, in ambito giudiziario (art. 46) e di polizia (art. 53) e dare attuazione ai principi del Codice relativamente ai trattamenti di dati effettuati per finalità di giustizia, di prevenzione o repressione di reati o di sicurezza pubblica (artt. 49 e 57). Tali provvedimenti, da tempo attesi e non ancora adottati malgrado le ripetute segnalazioni dell'Autorità (anche in considerazione della perdurante mancata attuazione della decisione quadro 2008/977/GAI sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale), sono di estrema importanza per completare il quadro normativo dei trattamenti in tali delicati ambiti (già di terzo pilastro), anche al fine di assicurare la corretta attuazione della normativa europea e internazionale;

Legge di delegazione europea 2013

4) la legge 7 ottobre 2014, n. 154, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea (legge di delegazione europea 2013 – secondo semestre). Fra gli atti cui il Governo è chiamato a dare attuazione rilevano, per gli aspetti di protezione dei dati personali, la decisione quadro 2006/960/GAI, relativa alla semplificazione dello scambio di informazioni e *intelligence* tra le Autorità degli Stati UE e la direttiva 2013/37/UE di modifica della direttiva 2003/98/CE relativa al riutilizzo dell'informazione nel settore pubblico (artt. 1, 6 e all. A);

Processo esecutivo e accesso a banche dati

5) il decreto-legge 12 settembre 2014, n. 132, convertito dalla legge 10 novembre 2014, n. 162, recante misure urgenti di degiurisdizionalizzazione ed altri interventi per la definizione dell'arretrato in materia di processo civile. Le disposizioni di maggior interesse sotto il profilo della protezione dei dati personali riguardano misure per l'efficienza e la semplificazione delle procedure di esecuzione forzata a tutela del creditore (art. 19). Con modifiche al codice di procedura civile (in particolare con il nuovo art. 492-*bis*) e alle relative disposizioni di attuazione sono state introdotte norme per consentire la ricerca con modalità telematiche dei beni da pignorare presso il debitore e presso terzi, al fine di colmare l'asimmetria informativa tra i creditori e il debitore in merito agli *asset* patrimoniali di quest'ultimo. In particolare, previa autorizzazione dell'autorità giudiziaria, su istanza del creditore procedente, l'ufficiale giudiziario può avere accesso mediante "collegamento telematico diretto" ai "dati contenuti nelle banche dati delle pubbliche amministrazioni o alle quali le stesse possono accedere" e, tra questi, a quelli contenuti nell'Anagrafe tributaria, compreso l'archivio dei rapporti finanziari, nel pubblico registro automobilistico nonché negli archivi degli enti previdenziali. L'accesso è consentito al fine di acquisire tutte le informazioni rilevanti per l'individuazione delle cose e dei crediti da sottoporre ad esecuzione, ivi comprese quelle concernenti i rapporti del debitore con istituti di credito, datori di lavoro o committenti. La disposizione normativa attende di essere resa esecutiva mediante decreto del Ministro della giustizia, da adottare sentito il Garante, con il quale dovranno essere individuati "i casi, i limiti e le modalità di esercizio della facoltà di accesso alle banche dati [...] nonché le modalità di trattamento e conservazione dei dati e le cautele a tutela della riservatezza dei debitori", come pure "le ulteriori banche dati delle pubbliche amministrazioni o alle quali le stesse possono accedere" che l'ufficiale giudiziario può interrogare (nuovo art. 155-*quater* disp. att. c.p.c.). La formulazione della disposizione di

rango primario è alquanto generica, sia perché non reca alcuna specificazione volta a circoscrivere in concreto i dati acquisibili ("tutte le informazioni rilevanti"), sia perché non individua le banche dati oggetto di possibile accesso (l'elenco riportato è solo esemplificativo e si fa riferimento anche a, non meglio precisati, ulteriori archivi cui le stesse amministrazioni "titolari" di banche dati possono a loro volta accedere). Sotto questo punto di vista, quindi, appare quanto mai importante la fase di attuazione della norma, in cui il Garante, nell'esprimere il parere sullo schema di decreto, potrà valutarne la conformità anzitutto ai principi di necessità e finalità del trattamento nonché di pertinenza e non eccedenza dei dati (artt. 3 e 11 del Codice). Rileva, infine, la disposizione in base alla quale il "Ministro della giustizia" può procedere al trattamento dei dati acquisiti senza necessità dell'informativa di cui all'art. 13 del Codice (art. 155-*quater*, secondo comma, disp. att. c.p.c.). La norma appare superflua alla luce del disposto degli artt. 46 e 47 del Codice che già esentano il Ministero della giustizia, come del resto gli uffici giudiziari, dall'obbligo di rendere l'informativa per i trattamenti effettuati per ragioni di giustizia;

Semplificazione, trasparenza e autorità indipendenti

6) il decreto-legge 24 giugno 2014, n. 90, recante misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari, convertito, con significative modificazioni e integrazioni, dalla legge 11 agosto 2014, n. 114. In merito, di particolare importanza per l'Autorità sono:

a) le misure tese a razionalizzare costi e funzioni delle "autorità indipendenti" (art. 22). In particolare: si esclude la possibilità che i componenti delle autorità indipendenti indicate nella disposizione – e tra esse il Garante –, alla scadenza del mandato, possano essere nominati presso altra autorità nei cinque anni successivi alla cessazione dell'incarico (il testo originario del decreto prevedeva due anni); le procedure concorsuali per il reclutamento del personale devono essere "gestite unitariamente", previa stipula di apposite convenzioni che assicurino, fra l'altro, la "specificità delle professionalità di ciascun organismo" (comma 4); le autorità devono ridurre il trattamento economico accessorio del personale in misura non inferiore al 20 % e la spesa per incarichi di consulenza, studio e ricerca e per gli organi collegiali non previsti dalla legge in misura non inferiore al 50 % rispetto a quella sostenuta nel 2013 (commi 5 e 6); devono altresì provvedere alla gestione unitaria dei servizi strumentali mediante la stipula di convenzioni o la costituzione di uffici comuni almeno tra due autorità ed, entro il 31 dicembre 2014, per almeno tre servizi (comma 7); le autorità sono assoggettate alle disposizioni in materia di acquisti centralizzati della p.a. (art. 1, commi 449 e 450, l. 27 dicembre 2006, n. 296) (comma 8); sono individuati i criteri ai quali attenersi nella gestione delle spese per gli immobili, il cui rispetto deve essere assicurato entro un anno dall'entrata in vigore della legge di conversione, dandone conto nelle successive relazioni annuali, che devono essere trasmesse anche alla Corte dei conti (commi 9 e 9-*bis*) (per le iniziative già poste in essere dal Garante, cfr. par. 25.2);
b) le modifiche apportate all'ambito soggettivo di applicazione del d.lgs. 14 marzo 2013, n. 33, in materia di trasparenza amministrativa, con la sostituzione integrale dell'art. 11 (art. 24-*bis*, d.l. n. 90/2014). In base alla previgente formulazione, tra i destinatari degli obblighi di pubblicazione figuravano, oltre alle amministrazioni di cui all'art. 1, comma 2, d.lgs. n. 165/2001, anche le autorità indipendenti che dovevano provvedere ad attuare la normativa in materia di trasparenza "secondo le disposizioni dei rispettivi ordinamenti". Il novellato art. 11 precisa, invece, che nella nozione di "pubbliche amministrazioni" – cui si applica il menzionato d.lgs. n. 33 –

rientrano anche le autorità amministrative indipendenti di garanzia, vigilanza e regolazione, alle quali, pertanto, le norme in materia di trasparenza si applicano, ora, in via diretta ed immediata (per l'adeguamento alla disciplina posta in essere dal Garante, v. par. 24.2);

c) la rideterminazione delle funzioni dell'Autorità nazionale anticorruzione (Anac), anche a seguito della soppressione dell'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture, i cui compiti e funzioni sono trasferiti all'Anac. Per quanto di interesse del Garante, si segnala l'attribuzione all'Anac del potere sanzionatorio in caso di omessa adozione da parte delle amministrazioni degli atti di pianificazione in materia di trasparenza (programma triennale) nonché il compito di ricevere notizie e segnalazioni di illeciti (art. 19, comma 5). Il Presidente dell'Anac è tenuto altresì a segnalare all'autorità amministrativa competente in base alla l. n. 689/1981 le violazioni in materia di comunicazioni di dati e informazioni e di pubblicazione obbligatoria espressamente sanzionate ai sensi del d.lgs. n. 33/2013 (art. 19, comma 7; artt. 14, 22 e 47, d.lgs. n. 33/2013). Infine, sono trasferite all'Anac le funzioni (già attribuite dall'art. 48, d.lgs. n. 33/2013 al Dipartimento della funzione pubblica) concernenti la definizione di criteri, modelli e schemi *standard* per l'organizzazione, la codificazione e la rappresentazione dei documenti, delle informazioni e dei dati oggetto di pubblicazione obbligatoria, nonché per l'organizzazione della sezione "Amministrazione trasparente" dei siti istituzionali;

d) alcune disposizioni che apportano modifiche al d.lgs. n. 82/2005 recante il codice dell'amministrazione digitale (Cad) o ne disciplinano gli aspetti applicativi. Per finalità di semplificazione, si prevede che le regole tecniche per l'attuazione dell'Agenda digitale italiana siano stabilite secondo la procedura prevista dall'art. 71 del Cad che, contestualmente, viene modificata, stabilendosi in 30 giorni il termine entro il quale le amministrazioni competenti, la Conferenza unificata e il Garante devono esprimere il proprio parere, decorso il quale lo si intende favorevolmente espresso (art. 24-*ter*). Sono sanzionate le pp.aa. che non rispettano alcuni obblighi previsti dal Cad (obbligo di usare esclusivamente i canali e i servizi telematici, ivi inclusa la posta elettronica certificata, per l'utilizzo dei propri servizi, anche a mezzo di intermediari abilitati, nonché per la presentazione da parte degli interessati di denunce, istanze e altri atti, *ex* art. 63; pubblicazione nel proprio sito web, all'interno della sezione «Trasparenza, valutazione e merito», del catalogo dei dati, dei metadati e delle relative banche dati, nonché dei regolamenti che disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo delle informazioni *ex* art. 52, comma 1). Particolarmente importante – anche in relazione ai compiti istituzionali rimessi al Garante – è la previsione secondo cui i soggetti cui si applica il Cad (le pp.aa. di cui all'art. 1, comma 2, d.lgs. n. 165/2001, nonché le società interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della p.a.) devono comunicare all'AgID, esclusivamente per via telematica, l'elenco delle "basi di dati" in loro gestione e degli applicativi che le utilizzano. Ciò consente di censire presso l'AgID tutte le basi di dati "in mano pubblica" e relativi applicativi (art. 24-*quater*). Di rilievo è anche l'integrale riscrittura dell'art. 58 del Cad (art. 24-*quinquies*), il cui comma 2, come è noto, nel testo previgente prevedeva che le amministrazioni titolari di banche di dati accessibili per via telematica predisponessero con-

venzioni con le amministrazioni interessate all'accesso alle informazioni necessarie per accertamenti d'ufficio o per il controllo delle autodichiarazioni rese dai cittadini, sulla base di Linee guida di Digit-Pa adottate previo parere del Garante (Linee guida per la stesura di convenzioni per la fruibilità di dati della pubblica amministrazione – giugno 2013). Tale disciplina è stata integralmente abrogata. In base al nuovo comma 2 dell'art. 58, eliminato il ricorso alle predette convenzioni, si è previsto che le pp.aa. comunichino "tra loro attraverso la messa a disposizione a titolo gratuito degli accessi alle proprie basi di dati alle altre amministrazioni mediante la cooperazione applicativa di cui all'art. 72" del medesimo Cad. In attuazione del novellato disposto normativo, l'AgID dovrà definire "gli *standard* di comunicazione e le regole tecniche a cui le pubbliche amministrazioni devono conformarsi", consultando nuovamente, a tal fine, il Garante affinché *standard* e "regole tecniche" comunque siano definiti in conformità alla disciplina sulla protezione dei dati, analogamente a quanto già prescritto in occasione dell'adozione delle Linee guida. La nuova disposizione normativa sembra avere una valenza generale, riferita cioè a tutti gli scambi informativi fra pp.aa, rispetto ai quali si limita a stabilire l'accesso "gratuito" delle pp.aa. alle rispettive banche dati e l'obbligo di conformarsi agli *standard* di comunicazione e alle regole tecniche che saranno adottati dall'AgID. In altri termini, deve ritenersi che la norma, in assenza di specifiche previsioni al riguardo, lasci impregiudicata l'applicazione della normativa in materia di protezione dei dati personali, segnatamente per quanto riguarda la disciplina dei presupposti e delle condizioni delle comunicazioni di dati fra soggetti pubblici (artt. 18-22 del Codice);

e) numerosi articoli del decreto-legge volti a dare completa attuazione al processo telematico che, almeno nel settore civile, è divenuto pienamente operativo a partire dal 30 giugno 2014. Il decreto si occupa del processo civile (ad es.: tempistica per il deposito telematico degli atti; previsione che le vendite di cose mobili pignorate debbano essere interamente effettuate con modalità telematiche, pur con alcune eccezioni), del processo amministrativo (si prevede, fra l'altro, che si applichino anche nel processo amministrativo le disposizioni relative alle comunicazioni e notificazioni per via telematica quando relative ai soggetti per i quali la legge prevede l'obbligo di munirsi di un indirizzo di posta elettronica certificata o alle pp.aa.) nonché del processo contabile (consentendo l'utilizzo di modalità telematiche anche nei giudizi contabili dinanzi alla Corte dei conti, purché sia garantita la "riservatezza dei dati personali"). A quest'ultimo riguardo l'art. 43 del decreto stabilisce che le relative regole tecniche volte a disciplinare l'utilizzo della Pec per le notificazioni e comunicazioni processuali, nonché nella trasmissione degli atti, siano adottate con decreto del Presidente della Corte dei conti; sul relativo schema il Garante ha recentemente espresso il proprio parere di competenza (cfr. par. 3.4.1);

f) l'interpolazione dell'art. 62, comma 3, del Cad con la previsione secondo cui i comuni possono svolgere le funzioni di competenza, "ad eccezione di quelle anagrafiche", utilizzando i dati anagrafici, costantemente allineati a quelli registrati nell'Anagrafe nazionale della popolazione residente (Anpr) conservati in "basi di dati locali" (art. 24, comma 4-*ter*). La disposizione assume importanza ai fini dell'attuazione della riforma delle anagrafi e dell'Anpr anche in relazione alle disposizioni del decreto di attuazione del

predetto art. 62 del Cad (d.P.C.M. 10 novembre 2014, n. 194), sul cui schema il Garante ha reso un parere condizionato in data 17 aprile 2014 (n. 202, doc. web n. 3105794) (cfr. par. 3.4.1);

g) in materia di Agenda della semplificazione amministrativa, la previsione dell'obbligo per le amministrazioni dello Stato di dotarsi di un piano di informatizzazione delle procedure di presentazione di istanze, dichiarazioni e segnalazioni (art. 24). La compilazione automatizzata dovrà avvenire tramite autenticazione con il Sistema pubblico dell'identità digitale (Spid), strumento previsto dall'articolo 64 del Cad (sul relativo schema di decreto il Garante ha reso parere in data 19 giugno 2014, n. 311, doc. web n. 3265492: cfr. par. 3.4.1);

Trasparenza

7) il decreto-legge 24 aprile 2014, n. 66, recante misure urgenti per la competitività e la giustizia sociale, convertito dalla legge 23 giugno 2014, n. 89, che introduce nuovi obblighi in materia di trasparenza. In particolare, l'art. 8, modificando gli artt. 29 e 33, d.lgs. n. 33/2013, prevede l'integrale pubblicazione dei bilanci di previsione e dei conti consuntivi delle pp.aa., in formato aperto che ne consenta il riutilizzo, nonché dei tempi medi di pagamento relativi agli acquisti di beni e forniture ("indicatore annuale di tempestività dei pagamenti"). Inoltre, per un verso, si fissa in 240.000 euro il "limite massimo retributivo" riferito al primo presidente della Corte di Cassazione e si prevede la sua applicazione anche agli emolumenti dei componenti degli organi di amministrazione, direzione e controllo delle autorità amministrative indipendenti (art. 13, comma 2, lett. *b*), che modifica l'art. 1, comma 472, l. 27 dicembre 2013, n. 147); per altro verso, si introduce per le pp.aa. inserite nel conto economico consolidato, l'obbligo di pubblicare i dati completi relativi ai compensi percepiti da ciascun componente del consiglio di amministrazione in qualità di componente di organi di società ovvero di fondi controllati o partecipati dalle amministrazioni stesse (art. 13, comma 5-*bis*);

Finanziamento dei partiti

8) il decreto-legge 28 dicembre 2013, n. 149, convertito, con modificazioni, dalla l. 21 febbraio 2014, n. 13, recante abolizione del finanziamento pubblico diretto, disposizioni per la trasparenza e la democraticità dei partiti e disciplina della contribuzione volontaria e della contribuzione indiretta in loro favore. Fra le disposizioni di interesse sotto il profilo della protezione dei dati personali si segnalano le seguenti: a) lo statuto dei partiti politici che intendono fruire dei benefici previsti dalla nuova legge deve contenere anche le regole per assicurare "il rispetto della vita privata e la protezione dei dati personali", la cui indicazione costituisce, quindi, una condizione di democrazia interna del partito (art. 3, comma 2, lett. o-*bis*); b) devono essere pubblicati nel sito internet del Parlamento i dati relativi alla situazione reddituale e patrimoniale dei titolari di cariche di governo e dei parlamentari, ai sensi di quanto prevede il d.lgs. n. 33/2013, e le relative dichiarazioni patrimoniali e di reddito (di cui alla l. n. 441/1982) devono essere corredate di tutti i finanziamenti privati ricevuti a titolo di liberalità (direttamente o a mezzo di comitati di sostegno) di importo superiore a 5.000 euro l'anno; anche di tali dichiarazioni è data evidenza nel sito internet del Parlamento, quando sono pubblicate nel sito del rispettivo ente (art. 5, commi 2 e 2-*bis*); c) in relazione ai finanziamenti o ai contributi erogati in favore dei partiti politici iscritti nell'apposito registro, deve essere trasmesso alla Presidenza della Camera, a cura dei rappresentanti legali dei partiti che ne beneficiano, l'elenco degli erogatori di somme superiori nell'anno ai 5.000 euro, con la relativa documentazione contabile, suscettibile di pubblicazione nel sito del Parlamento nonché nel sito del partito (art. 5, comma 3). Al riguardo, sulla scorta della segnalazione del Garante al Parlamento e al Governo sull'argomento (per la quale si veda *amplius* il par. 3.1), la pubblicazione dei dati dei sovventori è limitata ai soli soggetti che abbiano prestato

il proprio consenso specifico alla pubblicazione *online* dei dati personali sensibili, ai sensi degli artt. 22, comma 12, e 23, comma 4, del Codice; d) è ora possibile destinare il due per mille dell'imposta individuale sul reddito delle persone fisiche in favore di un partito politico che soddisfi le condizioni previste per poter beneficiare di tale forma di finanziamento; per l'attuazione di tale nuovo meccanismo di contribuzione sono stati adottati il d.P.C.M. 28 maggio 2014 (recante, fra l'altro, le modalità di semplificazione degli adempimenti e di tutela della riservatezza nonché di espressione delle scelte preferenziali dei contribuenti, sul cui schema il Garante ha reso il parere 22 maggio 2014, n. 256, doc. web n. 3246663: cfr. par. 3.4.1) e il provvedimento 3 aprile 2014 dell'Agenzia delle entrate, recante la disciplina transitoria per il primo anno di applicazione della nuova normativa (sul quale pure il Garante ha reso parere 3 aprile 2014, n. 166, doc. web n. 3104253) (art. 12, commi 3 e 3-*bis*); e) le raccolte telefoniche di fondi per campagne promozionali di partecipazione alla vita politica (attraverso sms, altre applicazioni da telefoni mobili o chiamate in fonia da utenze di telefonia fissa) sono sottoposte ad un apposito codice di autoregolamentazione tra i gestori telefonici autorizzati (art. 13); f) mediante modifica dell'art. 12, l. 6 luglio 2012, n. 96, concernente la pubblicità della situazione patrimoniale e reddituale dei soggetti che svolgono le funzioni di tesoriere dei partiti o dei movimenti politici o funzioni analoghe, si limita l'applicabilità delle norme in materia di pubblicità ai soli tesorieri dei partiti che abbiano almeno un rappresentante eletto in Parlamento; le disposizioni sulla pubblicità sono state, invece, estese ai membri del partito che assumono il ruolo di responsabile o rappresentante nazionale, componente dell'organo di direzione politica nazionale, presidente di organi nazionali deliberativi o di garanzia (art. 15).

2.1.2. I decreti legislativi

Quanto alla normativa primaria delegata, si segnalano, fra i decreti di maggior interesse, i seguenti:

a) il decreto legislativo 17 aprile 2014, n. 70, recante disciplina sanzionatoria per le violazioni delle disposizioni del regolamento (CE) 1371/2007, relativo ai diritti e agli obblighi dei passeggeri nel trasporto ferroviario, che prevede, all'art. 11, comma 2, l'obbligo dell'organismo di controllo (Autorità di regolazione dei trasporti) di informare tempestivamente il Garante in caso di inosservanza del divieto di fornire informazioni personali su singole prenotazioni ad altre imprese ferroviarie o a venditori di biglietti (art. 10, par. 5, reg. (CE) 1371/2007);

b) il decreto legislativo 4 marzo 2014, n. 37, di attuazione della direttiva 2011/82/UE intesa ad agevolare lo scambio transfrontaliero di informazioni sulle infrazioni in materia di sicurezza stradale, per il quale si rimanda a quanto descritto in relazione al parere reso dal Garante sul relativo schema di decreto (cfr. par. 3.4.2). È interessante, in questa sede, rilevare che con sentenza del 6 maggio 2014, Commissione europea c. Parlamento europeo e Consiglio dell'Unione europea (causa C-43/12), la CGUE ha annullato la direttiva in questione, ritenendo che la stessa avrebbe dovuto essere adottata sulla base dell'art. 91 Trattato sul funzionamento dell'Unione europea (TFUE), vista la finalità di miglioramento della sicurezza dei trasporti, piuttosto che *ex* art. 87 TFUE nell'ambito della cooperazione di polizia. Nonostante l'annullamento, per ragioni di certezza del diritto (essendo peraltro già decorso il termine per il recepimento negli ordinamenti nazionali, fissato per il 7 novembre 2013), la Corte ha stabilito che gli effetti della direttiva siano comunque mantenuti per il termine massimo di un

anno. L'11 marzo 2015 è stata adottata la nuova direttiva 2015/413/UE mirante a favorire lo scambio transfrontaliero di informazioni sulle infrazioni in materia di sicurezza stradale;

Minori

c) il decreto legislativo 4 marzo 2014, n. 39, recante recepimento della direttiva 2011/93/UE in materia di lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile (che sostituisce la decisione quadro 2004/68/GAI). Mediante modifiche al codice penale (cfr. art. 602-*ter* come integrato e nuovo art. 609-*duodecies*) si introduce una specifica aggravante nei casi in cui numerosi reati contro i minori fra quelli previsti nel Titolo XII, capo III del codice penale siano compiuti "con l'utilizzo di mezzi atti ad impedire l'identificazione dei dati di accesso alle reti telematiche" (art. 1). Inoltre si integra il d.P.R. n. 313/2002 con l'art. 25-*bis*, in base al quale il datore di lavoro che intenda impiegare una persona per lo svolgimento di attività professionali o volontarie organizzate che comportino contatti diretti e regolari con minori, deve richiedere il certificato penale del casellario giudiziale rilasciabile a richiesta dell'interessato, al fine di verificare l'esistenza di condanne per taluno dei predetti reati contro i minori o l'irrogazione di sanzioni interdittive all'esercizio di attività che comportino contatti diretti e regolari con minori (art. 2);

Assistenza sanitaria transfrontaliera

d) il decreto legislativo 4 marzo 2014, n. 38, recante attuazione della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera nonché della direttiva 2012/52/UE comportante misure destinate ad agevolare il riconoscimento delle ricette mediche emesse in un altro Stato membro. La disposizione di maggiore interesse per l'Autorità è rappresentata dall'art. 11, comma 4, secondo la quale, anche al fine di dare piena attuazione al principio di mutua assistenza e cooperazione tra Stati in materia di assistenza sanitaria transfrontaliera, il Ministero della salute – attraverso la revisione del flusso informativo relativo alle schede di dimissione ospedaliera (sdo) e in osservanza di quanto previsto in punto di interconnessione dei sistemi informativi e di codifica dei dati (art. 15, comma 25-*bis*, d.l. n. 95/2012) – promuove un sistema di monitoraggio delle attività e delle reti assistenziali che permetta la rilevazione degli *standard* di qualità e di sicurezza della rete ospedaliera nonché dei volumi e degli esiti delle cure erogate dai prestatori di assistenza sanitaria.

3 I rapporti con il Parlamento e le altre Istituzioni

3.1. *Le segnalazioni al Parlamento e al Governo*

Nel corso del 2014 il Garante – nell'espletamento delle proprie attribuzioni – ha in più occasioni segnalato al Parlamento e al Governo l'opportunità di interventi normativi volti ad assicurare le dovute tutele ai diritti degli interessati e in particolare al diritto alla protezione dei dati personali, anche in relazione all'evoluzione registrata in determinati settori (art. 154, comma 1, lett. *f*), del Codice), segnatamente con riguardo alle seguenti tematiche:

a) Disposizioni in materia di accesso ai dati concernenti le proprie origini

La più recente segnalazione si è incentrata sull'AC 784 (e abbinate) "Disposizioni in materia di accesso del figlio adottato non riconosciuto alla nascita alle informazioni sulle proprie origini e sulla propria identità", all'esame della Commissione giustizia della Camera dei deputati. In risposta ad una specifica richiesta della predetta Commissione, il Garante ha fornito al Parlamento alcuni elementi di riflessione e valutazione utili a conformare la disciplina in questione ai principi e alle regole in materia di protezione dei dati personali e, in particolare, alle vigenti garanzie per l'anonimato della madre che non abbia riconosciuto il figlio (nota 25 settembre 2014, doc. web n. 3847799).

La tutela della riservatezza dell'identità delle madri che al momento del parto si sono avvalse del diritto di non essere nominate è attualmente prevista dal combinato disposto dell'art. 28, comma 7, l. 4 maggio 1983, n. 184 (come modificato dall'art. 177, comma 2, del Codice) e dall'art. 30, comma 1, d.P.R. 3 novembre 2000, n. 396. Analogamente, l'art. 93 del Codice prevede che non possano essere resi noti, se non decorsi cento anni dalla formazione del documento, il certificato di assistenza al parto o la cartella clinica, a meno che in essi non vengano oscurati i dati personali che rendono identificabile la madre naturale che abbia esercitato il diritto a non essere nominata. Le summenzionate disposizioni assicurano la possibilità del cd. parto in anonimato al fine di tutelare il più possibile la salute della madre e la vita del nascituro, consentendo alla donna di partorire nella piena riservatezza, ma anche con la migliore assistenza possibile all'interno delle strutture ospedaliere.

Come è noto, nella sentenza n. 278/2013 la Corte costituzionale ha dichiarato l'illegittimità del citato art. 28, comma 7, nella parte in cui non prevede, attraverso un procedimento stabilito dalla legge, la possibilità per il giudice di interpellare la madre, su richiesta del figlio, al fine di una eventuale revoca della dichiarazione di non voler essere nominata.

Nella nota trasmessa al Parlamento, l'Autorità ha rilevato che la sentenza non ha scalfito il diritto alla riservatezza delle madri – avendo, al contrario, la Corte ribadito la necessità di proteggere l'anonimato delle donne "attraverso un procedimento, stabilito dalla legge, che assicuri la massima riservatezza" delle stesse – ed ha quindi richiamato l'attenzione della Commissione sulla necessità di un organico intervento normativo in grado di assicurare che il diritto dei figli a conoscere le proprie origini biologiche non vada a detrimento della riservatezza delle donne.

Quanto al merito della disciplina normativa, pur nella consapevolezza della complessità del bilanciamento dei diritti in campo, l'Autorità ha ritenuto praticabile la

proposta – emersa nel dibattito parlamentare – di una sorta di "registro delle revoche" o "registro delle identità materne", che alcuni esperti auditi dai membri della Commissione hanno ritenuto opportuno affidare ad un comitato *ad hoc* (sul modello francese, ove la sua tenuta è affidata ad un organo a composizione mista e paritetica, il *Conseil National pour l'accès aux origines personnelles*) o anche a questa Autorità, al fine di evitare problemi di coordinamento tra gli uffici dei tribunali sparsi sull'intero territorio nazionale.

L'istituzione di un registro con la conseguente tenuta centralizzata delle informazioni agevolerebbe l'intera procedura, assicurando uno *standard* di riservatezza più elevato, sia perché procedimentalizzerebbe univocamente alcuni passaggi, sia perché, presupponendo una scelta consapevole da parte della madre naturale, contribuirebbe ad una gestione più razionale e meno conflittuale dell'istanza di accesso del figlio. L'eventuale scelta di affidare al Garante la tenuta del registro sarebbe pienamente conforme con il quadro ordinamentale e normativo vigente e, in particolare, con le funzioni assegnate all'Autorità.

D'altra parte – come sancito dalla Corte – va garantita l'assoluta riservatezza anche della procedura di interpello della madre, da parte del giudice e su istanza del figlio, nelle diverse ipotesi in cui la donna non si sia iscritta nel "registro delle revoche". Anche in tal caso – ha concluso il Garante – si potrebbe valutare l'opportunità di assegnare all'Autorità la funzione di garanzia della riservatezza di tale procedura, ancor più delicata perché potrebbe coinvolgere donne che intendono mantenere l'anonimato.

b) Misure di semplificazione per i titolari del trattamento e razionalizzazione del quadro sanzionatorio previsto dal Codice

L'Autorità ha sottoposto all'attenzione del Governo alcune misure di semplificazione della normativa in materia di protezione dei dati personali volte a snellire gli adempimenti cui sono tenuti i titolari del trattamento e a razionalizzare il quadro sanzionatorio, senza tuttavia abbassare lo *standard* delle garanzie individuali e nel rispetto dei vincoli dell'Unione europea. Il progetto di riforma – inoltrato al Presidente del Consiglio dei ministri, al Ministro della giustizia e al Ministro per la semplificazione e la pubblica amministrazione, con note del 22 settembre 2014 (doc. web n. 3531329) – si ispira ai seguenti principi:

- semplificazione del quadro sanzionatorio previsto dal Codice e aumento dell'equità nell'applicazione delle sanzioni, mediante, fra l'altro, la ridefinizione dei confini tra le fattispecie penali e amministrative e la limitazione della responsabilità penale per la mancata adozione delle misure minime di sicurezza ai soli casi in cui ne sia derivata una conseguenza per gli interessati;
- riduzione dei costi diretti e indiretti (di consulenza e assistenza legale) per i soggetti destinatari di sanzioni, mediante il ricorso automatico a modalità di estinzione agevolata dei procedimenti sanzionatori e riducendo i casi in cui non è ammessa l'estinzione mediante oblazione;
- promozione di un aggiornamento delle misure minime di sicurezza previste dal Codice (art. 36) anche con disposizioni differenziate in ragione dei rischi effettivi per i diritti degli interessati e minimizzando l'impatto economico delle stesse, in particolare presso le piccole e medie imprese, liberi professionisti e artigiani. A tal fine, si prevede la consultazione delle categorie interessate e si affida al Garante il compito di proporre tali adempimenti sulla base dell'esperienza maturata dalla quotidiana applicazione delle relative disposizioni.

Al riguardo il Ministro della giustizia ha assicurato che il contributo del Garante sarà tenuto nella dovuta considerazione, preferibilmente con il coinvolgimento del Parlamento ed eventualmente mediante il ricorso alla delega legislativa, attesa la necessità di garantire il corretto equilibrio fra la tutela dei diritti degli utenti e le esigenze di semplificazione per le imprese, anche in relazione agli sviluppi in sede europea dell'esame delle proposte di regolamento e di nuova direttiva (cd. pacchetto *privacy*).

c) La riforma del finanziamento dei partiti politici

Il Garante ha presentato al Parlamento e al Governo una segnalazione in relazione ad una previsione del d.l. 28 dicembre 2013, n. 149, recante la riforma del finanziamento dei partiti politici (nota 7 febbraio 2014, doc. web n. 3523017, inoltrata alla Commissione affari costituzionali del Senato, cui era rimesso l'esame del disegno di legge di conversione del decreto, al Presidente del Senato e al Ministro per i rapporti con il Parlamento). Premesso che delle disposizioni di interesse sotto il profilo della protezione dei dati contenute nel provvedimento d'urgenza, dopo la sua conversione in legge, si è già dato conto (cfr. paragrafo 2.1.1), l'art. 5 del decreto prevedeva che i partiti politici comunicassero alla Presidenza della Camera dei deputati l'elenco dei soggetti eroganti finanziamenti o contributi di importo superiore, nell'anno, a euro 5.000, e che detto elenco venisse pubblicato, unitamente agli importi erogati, sul sito internet dei partiti politici e del Parlamento. Atteso che la menzionata disposizione avrebbe comportato una diffusione di dati personali sensibili, idonei cioè a rivelare le opinioni politiche delle persone, tale operazione avrebbe dovuto implicare l'adozione delle particolari garanzie previste dal Codice e, in particolare, il rilascio del previo consenso scritto degli interessati (artt. 4, comma 1, lett. *d*) e *m*), e 26 del Codice). Con la segnalazione, il Garante ha chiesto, pertanto, di valutare l'opportunità di non derogare al principio generale in materia di trattamento di dati sensibili che, attraverso l'istituto del consenso, rimette all'autodeterminazione e alla libera scelta dei singoli la possibilità o meno di diffondere i propri dati sensibili. Ne è scaturito un emendamento che ha tenuto conto delle osservazioni dell'Autorità e ha subordinato al consenso degli interessati la pubblicazione dei dati nei siti internet dei partiti politici e nel sito internet ufficiale del Parlamento italiano (cfr. ora l'art. 5 come modificato dalla l. 21 febbraio 2014, n. 13 di conversione).

d) Disposizioni normative in materia di utilizzo della cd. scatola nera

Un'altra segnalazione ha riguardato un'iniziativa legislativa in materia di riduzione dei premi di assicurazione r.c. auto (art. 8, d.l. 23 dicembre 2013, n. 145), con la quale si intendeva integrare l'art. 132 del codice delle assicurazioni private (d.lgs. n. 209/2005) nella parte relativa alla possibilità per le imprese di assicurazione di proporre la stipula di contratti con l'installazione di meccanismi elettronici che registrano l'attività del veicolo, denominati "scatola nera" (o altri dispositivi individuati con il d.m. 25 gennaio 2013, n. 5). L'art. 8 del provvedimento d'urgenza, nell'intento di introdurre un nuovo modello organizzativo della "portabilità" degli apparati, stabiliva che la "interoperabilità" dei meccanismi elettronici che registrano l'attività del veicolo fosse garantita dal Ministero delle infrastrutture e dei trasporti attraverso un "servizio unico di raccolta dei dati", eventualmente affidato in concessione, da costituirsi presso le strutture tecniche del Centro di coordinamento delle informazioni sul traffico, sulla viabilità e sulla sicurezza stradale (Cciss). In sostanza la disposizione individuava in un organismo pubblico il soggetto titolare delle funzioni e delle responsabilità ai fini dell'interoperabilità, stabilendo che i dati registrati dai dispositivi fossero trasferiti al Cciss e da questi – anche tramite concessionario – resi poi disponibili alle compagnie di assicurazioni. Al riguardo, il Garante, in rispo-

sta ad una specifica richiesta della X Commissione attività produttive, commercio e turismo della Camera dei deputati, innanzi alla quale era in discussione il disegno di legge di conversione del decreto, ha ritenuto di fornire elementi di valutazione sulle possibili implicazioni in materia di protezione dei dati personali della disciplina proposta (nota 24 gennaio 2014, doc. web n. 3825619). Pur condividendo la finalità (contenere i costi dell'assicurazione r.c. auto) sottesa alla disposizione, il Garante ha evidenziato come la stessa non chiarisse gli ambiti di responsabilità dei soggetti coinvolti nel sistema (l'organismo pubblico citato, il concessionario del servizio e le stesse imprese di assicurazione) né, soprattutto, definisse le informazioni suscettibili di essere raccolte dall'organismo pubblico, aspetto di fondamentale importanza, posto che il modello prospettato avrebbe potuto determinare la centralizzazione di una notevole quantità di informazioni (e, tra queste, quelle relative alla localizzazione dei veicoli). Si è ritenuto che anche la questione dell'interoperabilità, sotto il profilo della standardizzazione dei formati dei dati generati dalle *black box* e di altri parametri del loro funzionamento, dovesse essere affrontata in altra sede, potendo rappresentare – soprattutto in chiave futura – una valida alternativa alla raccolta centralizzata delle informazioni. L'art. 8 in parola non è stato confermato dalla legge di conversione 21 febbraio 2014, n. 9 (emendamento 8.100 soppressivo dell'articolo in questione, in seduta 5 febbraio 2014 delle Commissioni riunite VI finanze e X attività produttive della Camera).

3.2. *Le audizioni del Garante in Parlamento*

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

a) un'audizione tenutasi il 3 dicembre 2014 presso la Commissione giustizia della Camera dei deputati nell'ambito dei lavori su alcune proposte di legge in materia di diffamazione, anche con il mezzo della stampa o con altro mezzo di diffusione, di ingiuria e di segreto professionale. Prendendo spunto da una norma dell'articolato (AC 925-B) che disciplina il diritto alla rimozione, dai siti internet e dai motori di ricerca dei contenuti diffamatori e dei dati personali trattati in violazione di legge, il Garante ha auspicato una più ampia riflessione del Parlamento sull'opportunità di disciplinare compiutamente – eventualmente in un testo normativo più generale – il cd. diritto all'oblio, già previsto dallo proposta di regolamento europeo sulla protezione dei dati personali e che sta assumendo un'importanza sempre maggiore nel rapporto fra dignità e riservatezza dell'individuo, da un lato, e libertà di espressione, dall'altro;
b) un'audizione tenutasi il 23 settembre 2014 presso la Commissione lavoro pubblico e privato della Camera dei deputati nell'ambito dell'indagine conoscitiva sui rapporti di lavoro presso i *call center* presenti sul territorio italiano. Il Garante ha affrontato i delicati profili del trasferimento dei dati all'estero e del rispetto delle garanzie per gli interessati nonché delle connesse responsabilità dei titolari del trattamento nel caso in cui le imprese si avvalgano, per la loro attività promozionale, di *call center* situati in Paesi terzi, anche ai sensi dell'art. 24-*bis*, d.l. n. 83/2012 (conv. dalla l. n. 134/2012). Il documento conclusivo dell'indagine approvato l'11 dicembre 2014 dà risalto alle osservazioni del Garante e, in particolare, alla pro-

posta di introdurre nell'ordinamento una disposizione che attribuisca espressamente al soggetto per conto del quale si effettua il contatto promozionale la titolarità del trattamento dei dati, in modo che, in caso di trattamento illecito, ne discenda la responsabilità solidale con la società che effettua le chiamate. Siffatta previsione dovrebbe indurre le società committenti a delegare l'attività promozionale a soggetti affidabili e in grado di rispettare la normativa in materia di protezione dei dati personali;

c) un'audizione tenutasi il 23 luglio 2014, presso la Commissione igiene e sanità del Senato nell'ambito dell'indagine conoscitiva sulle origini e gli sviluppi del cd. caso Stamina. Prendendo spunto dal dibattito seguito alla nota vicenda – che ha toccato picchi di "accanimento informativo" sino alla divulgazione dell'immagine "in chiaro" di una bimba malata –, il Garante ha formulato alcune considerazioni sull'incompatibilità di un certo modo di fare informazione con la disciplina posta a tutela della riservatezza, che si risolve nella violazione della dignità e del diritto del minore a non vedere esibita la propria identità e infermità (anche alla luce della Carta di Treviso e del codice deontologico dei giornalisti);

d) un'audizione informale, tenutasi il 29 maggio 2014 presso la Commissione affari costituzionali, della Presidenza del Consiglio e interni della Camera dei deputati in merito alla proposta di legge che modifica l'art. 24, l. 7 agosto 1990, n. 241, in materia di accesso dei membri del Parlamento ai documenti amministrativi per esigenze connesse allo svolgimento del mandato parlamentare (AC 1761).

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

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

a) un'interrogazione sugli *standard* di sicurezza nel trattamento dei dati da parte dei *social network* e in particolare di *Facebook* (n. 4-01112 dell'on. Bianconi: nota 18 dicembre 2014);

b) un'interrogazione sul cd. *datagate* (interrogazione a risposta scritta n. 4-04805 dell'on. Prodani: nota 30 ottobre 2014), tema sul quale l'Autorità già nel 2013 ha avuto modo di esprimersi in relazione a ben quattro atti di sindacato ispettivo presentati in Parlamento sull'argomento (cfr. Relazione 2013, p. 22);

c) un'interrogazione sulle modalità di rilascio del cud da parte dell'Inps (interrogazione a risposta in Commissione n. 5-02313, dell'on. Garavini: nota 4 agosto 2014);

d) tre mozioni concernenti l'impatto sulla protezione dei dati personali dell'accordo commerciale internazionale di partenariato transatlantico per il commercio e gli investimenti (TTIP) (mozione 1-00558 dell'on. Kronblicher: nota 8 agosto 2014; mozione n. 1-00490 dell'on. Gallinella: nota 24 giugno 2014; mozione 1-00413 dell'on. Migliore: nota 28 maggio 2014);

e) una mozione e un'interrogazione concernenti il trattamento dei dati personali nell'attività di promozione commerciale svolta mediante *call center*, con particolare riferimento ai casi in cui il servizio è delocalizzato in Paesi

terzi in applicazione delle disposizioni dell'articolo 24-*bis*, d.l. n. 83/2012, convertito dalla l. n. 134/2012) (mozione n. 1-00457, dell'on. Palazzotto: nota 2 luglio 2014); interrogazione a risposta in Commissione lavoro della Camera n. 5-01719, dell'on. Albanella: nota 31 gennaio 2014);

f) una mozione in materia di *cyberbullismo* (n. 1-00233 dell'on. Ferrara ed altri: nota 13 giugno 2014).

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

3.4.1. I pareri sugli atti regolamentari e amministrativi del Governo

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

1) decreto del Ministro dell'interno recante modifiche al regolamento 21 giugno 2006, n. 244, per l'aggiornamento e l'integrazione dei tipi di dati sensibili e giudiziari e delle relative operazioni di trattamento effettuate dal Ministero dell'interno, adottato ai sensi degli artt. 20, comma 2, e 21, comma 2, del Codice (parere 11 dicembre 2014, n. 582, doc. web n. 3708655);

2) decreto del Presidente della Corte dei conti recante le prime regole tecniche ed operative per l'utilizzo della posta elettronica certificata nei giudizi dinanzi alla Corte dei conti, adottato ai sensi dell'art. 20-*bis*, d.l. 18 ottobre 2012, n. 179, convertito dalla l. 17 dicembre 2012, n. 221 (parere 4 dicembre 2014, n. 556, doc. web n. 3624087);

3) provvedimento del Ministero del lavoro e delle politiche sociali recante il modello tipo della dichiarazione sostitutiva unica (Dsu), dell'attestazione riportante l'Isee e delle relative istruzioni per la compilazione (parere 6 novembre 2014, n. 495, doc. web n. 3515450);

4) convenzione-tipo tra l'ente gestore (Consap s.p.a.) e gli "aderenti diretti" al sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità (istituito dal d.lgs. 11 aprile 2011, n. 64), adottato ai sensi dell'art. 4, comma 3, del decreto del Ministro dell'economia e delle finanze 19 maggio 2014, n. 95, sul cui schema il Garante aveva reso a suo tempo parere (cfr. Relazione 2013, par. 3.2) (parere 9 ottobre 2014, n. 445, doc. web n. 3505427);

5) convenzione tra il Ministero dell'economia e delle finanze e taluni "aderenti indiretti" al medesimo sistema di prevenzione, sul piano amministrativo, delle frodi mediante furto d'identità, adottata ai sensi dell'art. 4, comma 2, del decreto del Ministro dell'economia e delle finanze 19 maggio 2014, n. 95 (parere 18 settembre 2014, n. 408, doc. web n. 3487835);

6) decreto del Ministro dell'economia e delle finanze concernente l'individuazione delle specifiche tecniche del sistema di conservazione informatica delle negoziazioni effettuate dagli esercenti l'attività di cambiavalute ai sensi dell'art. 17-*bis*, comma 4, d.lgs. 13 agosto 2010, n. 141 (parere 25 settembre 2014, n. 425, doc. web n. 3487879);

7) d.P.R. recante disposizione di attuazione della l. 30 giugno 2009, n. 85, concernente l'istituzione della banca dati nazionale del dna e del laboratorio centrale per la banca dati nazionale del dna (parere 31 luglio 2014, n. 389, doc. web n. 3616088) (par. 9.2);

8) decreto interministeriale del Ministro dello sviluppo economico e del Ministro delle infrastrutture e dei trasporti recante il regolamento per l'istituzione e il funzionamento dell'"archivio informatico integrato" di cui all'art. 21, d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221 (parere 24 luglio 2014, n. 378, doc. web n. 3320757);

9) d.P.C.M. recante il regolamento per l'attuazione dell'art. 21 (Esperti nazionali distaccati) della l. 24 dicembre 2012, n. 234, recante "Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea" (poi decreto 30 ottobre 2014, n. 184; parere 10 luglio 2014, n. 355, doc. web n. 3325197);

10) d.P.C.M. recante definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini ed imprese (Spid), nonché dei tempi e delle modalità di adozione del sistema Spid da parte delle pp.aa. e delle imprese (poi decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014; parere 19 giugno 2014, n. 311, doc. web n. 3265492);

11) decreto dirigenziale del Ministero della giustizia recante modifiche al decreto 5 dicembre 2012 concernente la consultazione diretta del sistema informativo del casellario giudiziale da parte delle pp.aa. e dei gestori di pubblici servizi, ai sensi dell'art. 39, d.P.R. n. 313/2002 (poi decreto 12 giugno 2014; parere 19 giugno 2014, n. 312, doc. web n. 3273289);

12) decreto interministeriale recante regole tecniche per la realizzazione e il funzionamento del sistema informativo nazionale per la prevenzione nei luoghi di lavoro (Sinp), nonché le regole per il connesso trattamento dei dati, ai sensi dell'art. 8, comma 4, d.lgs. 9 aprile 2008, n. 81 (parere 12 giugno 2014, n. 295, doc. web n. 3255963);

13) decreto interministeriale del Ministro dell'interno e del Ministro dell'economia e delle finanze recante disposizioni organizzative per la Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza e istituzione dell'ufficio per la sicurezza (*security manager*) (parere 5 giugno 2014, n. 279, doc. web n. 3246681);

14) d.P.C.M. recante definizione dei criteri e delle modalità di destinazione della quota pari al due per mille dell'imposta sul reddito delle persone fisiche, in base alla scelta del contribuente, a favore di partiti politici, adottato ai sensi dell'art. 12, comma 3, d.l. 28 dicembre 2013, n. 149 (conv. dalla l. 21 febbraio 2014, n. 13, poi decreto 28 maggio 2014; parere 22 maggio 2014, n. 256, doc. web n. 3246663);

15) d.P.C.M. in materia di Fascicolo sanitario elettronico, adottato ai sensi dell'art. 12, comma 7, d.l. 18 ottobre 2012, n. 179 e dell'art. 13, comma 2-*quater*, d.l. 21 giugno 2013, n. 69 (parere 22 maggio 2014, n. 261, doc. web n. 3230826);

16) decreto del Ministro della giustizia concernente regole tecniche e operative per lo svolgimento della vendita dei beni mobili e immobili con modalità telematiche nei casi previsti dal codice di procedura civile (art. 161-*ter* delle disposizioni per l'attuazione del codice di procedura civile) (parere 15 maggio 2014, n. 245, doc. web n. 3235478);

17) d.P.C.M. recante le modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (Anpr) e definizione del piano per il graduale subentro dell'Anpr alle anagrafi della popolazione residente (parere 17 aprile 2014, n. 202, doc. web n. 3105794);

18) decreto del Ministro della giustizia recante modifiche al regolamento 22 dicembre 2006, n. 306, in materia di trattamento dei dati sensibili e giudiziari da parte del Ministero della giustizia (poi decreto 24 luglio 2014, n. 123, in *G.U.* 26 agosto 2014, n. 197; parere 10 aprile 2014, n. 201, doc. web n. 3104282);

19) decreto del Ministro dell'istruzione, dell'università e della ricerca riguardante le modalità delle prove di ammissione al corso di laurea magistrale in medicina e chirurgia in lingua inglese per l'anno accademico 2014-2015 (poi decreto 21 febbraio 2014, in *G.U.* 12 marzo 2014, n. 59; parere 20 febbraio 2014, n. 82, doc. web n. 2972695);

20) 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 2014-2015 (poi decreto 5 febbraio 2014, in *G.U.* 7 marzo 2014, n. 55; parere 30 gennaio 2014, n. 38, doc. web n. 2924822);

21) decreto del Ministro del lavoro e delle politiche sociali concernente la costituzione presso l'Inps del Casellario dell'assistenza, adottato ai sensi dell'art. 13, comma, 4, d.l. 31 maggio 2010, n. 78, convertito, dalla l. 30 luglio 2010, n. 122 (parere 23 gennaio 2014, n. 26, doc. web n. 2922956);

22) regolamento recante "Disposizioni concernenti le modalità di funzionamento, accesso, consultazione e collegamento con il CED di cui all'art. 8 della legge 1 aprile 1981, n. 121, della Banca dati nazionale unica della documentazione antimafia, istituita ai sensi dell'art. 96 del decreto legislativo 6 settembre 2011, n. 159" (parere 30 gennaio 2014, n. 39, doc. web n. 2924878).

Diversamente da quanto accaduto negli anni precedenti, nel 2014 non si sono registrati casi di mancata consultazione del Garante in relazione a provvedimenti aventi un particolare impatto sulla protezione dei dati personali (ai sensi del medesimo art. 154, comma 4, del Codice). Ciò è, evidentemente, il segno di una accresciuta sensibilità delle pubbliche amministrazioni sulla protezione dei dati personali – frutto anche dell'approccio collaborativo dell'Autorità (sin dalla fase di elaborazione dei testi da sottoporre a parere) – e in particolare sull'utilità per le amministrazioni stesse del coinvolgimento dell'Autorità nella valutazione dei riflessi dei provvedimenti normativi sui diritti alla riservatezza e alla protezione dei dati delle persone.

3.4.2. I pareri su norme di rango primario

Su specifica richiesta del Governo il Garante ha inoltre reso parere su alcuni atti normativi del Governo aventi rango primario. L'art. 154, comma 4, del Codice, infatti, fa riferimento alla normativa avente rango secondario, anche se la correlata disposizione della direttiva europea non reca una distinzione al riguardo (art. 28, paragrafo 2). Le richieste di parere su atti primari si inquadrano in un contesto collaborativo che l'Autorità, come più volte segnalato alla Presidenza del Consiglio, auspica possa ulteriormente svilupparsi, nella consapevolezza che sia di grande utilità il coinvolgimento del Garante nella fase preparatoria di iniziative legislative, oltre che regolamentari, del Governo al fine di valutarne previamente l'impatto sulla protezione dei dati personali e sui diritti delle persone. I pareri hanno riguardato in particolare:

a) Scambio transfrontaliero di dati su infrazioni stradali

Uno schema di decreto legislativo di recepimento della direttiva 2011/82/UE in materia di scambio transfrontaliero di informazioni sulle infrazioni in materia di sicurezza stradale, adottato in attuazione della l. 6 agosto 2013, n. 96 e volto a consentire lo scambio fra Paesi appartenenti all'Unione europea delle informazioni relative ai veicoli (e al rispettivo proprietario o intestatario) con i quali è stata commessa un'infrazione stradale, fra quelle individuate nella direttiva, in uno Stato membro diverso da quello di immatricolazione (poi d.lgs. 4 marzo 2014, n. 37; parere 9 gen-

naio 2014, n. 2, doc. web n. 2904320). Lo schema di decreto è stato predisposto all'esito dei lavori di un tavolo tecnico istituito presso la Presidenza del Consiglio dei ministri-Settore legislativo del Ministro per gli affari europei, cui ha fornito, a richiesta, il proprio contributo anche l'Ufficio, per quanto riguarda gli aspetti di protezione dei dati personali. Lo schema poi sottoposto a parere dell'Autorità non presentava criticità. Di particolare importanza è l'art. 10 dello schema che attribuisce all'interessato (che può essere anche il cittadino di un altro Stato UE, che ha commesso un'infrazione in Italia) due "nuovi" diritti (non previsti, allo stato, dalla normativa vigente e in particolare dal Codice), e cioè il diritto di ottenere: 1) che i dati non vengano cancellati, ma solo conservati temporaneamente se vi sono fondati motivi di ritenere che la cancellazione possa compromettere un proprio legittimo interesse, e trattati ulteriormente solo per lo scopo che ne ha impedito la cancellazione; 2) che sia data evidenza (mediante un indicatore di validità) ai dati di cui l'interessato contesta l'esattezza (cd. diritto di *flag*). Tali diritti sono esercitati con le modalità previste dal Codice e tutelati ricorrendo al Garante o all'autorità giudiziaria. Oltre a tali diritti, l'art. 10 del decreto "conferma" gli altri diritti dell'interessato già previsti dal Codice (ad esempio: rettifica, cancellazione, informativa) nei limiti ivi stabiliti (ad es., l'informativa non è dovuta rispetto a trattamenti effettuati per finalità di prevenzione, accertamento o repressione di reati quali sono alcune fattispecie di infrazioni stradali oggetto della direttiva e del decreto: guida in stato di ebbrezza o sotto l'influsso di stupefacenti *ex* artt. 186, 186-*bis* e 187 del codice della strada). Queste disposizioni sono state introdotte in attuazione della decisione quadro 2008/977/GAI, del Consiglio del 27 novembre 2008, concernente la protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia in materia penale, richiamata espressamente nella direttiva quale parametro di conformità. Tale decisione, com'è noto, non risulta ancora attuata in Italia malgrado le ripetute sollecitazioni dell'Autorità; tuttavia il richiamo contenuto nella direttiva europea ne ha reso necessaria l'implementazione limitatamente allo scambio di informazioni sulle infrazioni stradali, al fine di evitare l'instaurazione di procedure d'infrazione per mancato recepimento della direttiva stessa. Nel parere, pertanto, l'Autorità ha segnalato alla Presidenza del Consiglio la complessità ed i rischi di una "attuazione parziale" della decisione quadro, per la difficoltà di adattare le disposizioni in materia di protezione dei dati personali in essa contenute – concepite, ovviamente, in relazione agli scambi informativi per ogni tipologia di cooperazione giudiziaria e di polizia – a scambi di dati in specifici settori.

b) Ordine di protezione europeo

Uno schema di decreto legislativo per il recepimento della direttiva europea 2011/99/UE in materia di "ordine di protezione europeo", la quale prevede un meccanismo di mutuo riconoscimento dell'efficacia di provvedimenti adottati in materia penale dalle competenti autorità giurisdizionali nazionali (misure di protezione), finalizzati alla protezione di vittime di reati rispetto al pericolo di condotte idonee a ledere i loro diritti fondamentali (vita, integrità fisica, psichica o sessuale, dignità e libertà personale), come ad esempio rapimenti, molestie, *stalking*. Lo schema di decreto legislativo regolamenta, sul piano processuale, i presupposti per il riconoscimento all'estero degli effetti di una misura di protezione adottata dalle autorità italiane nonché quelli necessari per il riconoscimento in Italia degli effetti di un provvedimento emesso da autorità di altri Stati membri. Anche in questo caso, l'Ufficio ha partecipato ad un tavolo di lavoro presso la Presidenza del Consiglio dei ministri fornendo il proprio contributo in vista del successivo parere dell'Autorità (parere 30 ottobre 2014, n. 481, doc. web n. 3657992). Anche in tale materia il Governo ha

ritenuto indispensabile provvedere ad un'attuazione "parziale" della medesima decisione quadro 2008/977/GAI, richiamata nel considerando 36 della direttiva, per non incorrere in una procedura d'infrazione, introducendo, in relazione agli scambi informativi in materia di ordine di protezione europeo, disposizioni analoghe a quelle contenute nel d.lgs. n. 37/2014 sulle infrazioni stradali, sopra descritte (v. punto a). Lo schema, infatti, all'art. 15, dopo avere previsto l'applicazione ai trattamenti di dati effettuati ai sensi del decreto delle disposizioni contenute nella Parte II, Titolo I del Codice (Trattamenti in ambito giudiziario), attribuisce all'interessato, con le opportune precisazioni rese necessarie dalla specificità della materia, i due "nuovi" diritti alla conservazione temporanea dei dati in luogo della cancellazione e alla "evidenza" dell'esercizio dei diritti stessi. Ovviamente, l'Autorità in occasione del parere ha rinnovato la forte preoccupazione per i rischi derivanti da una "attuazione parziale" della Decisione-quadro.

c) Appartenenza a gruppo linguistico

Uno schema di decreto legislativo in materia di dichiarazione di appartenenza o aggregazione al gruppo linguistico nella Provincia di Bolzano, volto a integrare l'art. 20-*ter*, d.P.R. 26 luglio 1976, n. 752 (recante norme di attuazione dello Statuto speciale della Regione Trentino-Alto Adige in materia di proporzionale negli uffici statali della provincia e di conoscenza delle due lingue nel pubblico impiego), introdotto dal d.lgs. 23 maggio 2005, n. 99. L'art. 20-*ter* prevede che, al fine di poter beneficiare, nei casi previsti, degli effetti giuridici derivanti dall'appartenenza o dall'aggregazione al gruppo linguistico, ogni cittadino maggiorenne non interdetto, residente nella provincia, ha facoltà di rendere in ogni momento una dichiarazione individuale nominativa di appartenenza ad uno dei tre gruppi linguistici italiano, tedesco e ladino (art. 20-*ter*, comma 1, d.P.R. n. 752/1976). Lo schema di decreto era volto ad estendere il vigente regime normativo ai cittadini non residenti nella Provincia di Bolzano, anche se appartenenti ad altro stato dell'Unione europea, nonché ai cittadini di Paesi terzi titolari del permesso di soggiorno CE per soggiornanti di lungo periodo. La Presidenza del Consiglio dei ministri aveva già inoltrato a suo tempo richiesta di parere su una analoga proposta integrativa dell'art. 20-*ter*, che si riferiva però ai soli cittadini di altro stato dell'Unione europea. Nell'esprimere parere favorevole su tale precedente schema di decreto (parere 10 gennaio 2008) il Garante si era limitato a prendere atto della scelta allora operata dall'Amministrazione di non prendere in considerazione nella predetta estensione i cittadini appartenenti a Paesi terzi. L'Autorità, pertanto, non riscontrando nel testo ulteriori aspetti di criticità sotto il profilo della protezione dei dati personali, ha confermato l'avviso favorevole già espresso a suo tempo (parere 10 luglio 2014, n. 354, doc. web n. 3320726).

3.5. *L'esame delle leggi regionali*

È proseguita l'attività di esame del Garante delle leggi regionali approvate e sottoposte al vaglio di costituzionalità del Governo ai sensi dell'art. 127 della Costituzione, al fine di fornire alla Presidenza del Consiglio dei ministri eventuali elementi di valutazione circa la compatibilità delle stesse con le disposizioni in materia di protezione dei dati personali e con il dettato costituzionale (art. 117, comma 2, lett. *l*), Cost.). L'Autorità, nel corso dell'anno, ha esaminato 16 leggi regionali e, in linea generale, ha riscontrato un sostanziale corretto svolgimento della potestà legislativa regionale in relazione agli aspetti di protezione dei dati personali.

Solo in un caso sono stati forniti alla Presidenza del Consiglio elementi da valutare ai fini di una eventuale illegittimità costituzionale delle disposizioni normative e precisamente in relazione alla legge della Regione Calabria 18 dicembre 2013, n. 53, recante Disciplina del sistema regionale dell'istruzione e formazione professionale (nota 4 febbraio 2014).

Le osservazioni hanno riguardato l'art. 14 della legge che istituisce l'"anagrafe regionale degli studenti" (Ans), alimentata dalle informazioni sui percorsi degli studenti a partire dal primo anno della scuola primaria e "coordinata ed integrata" con l'anagrafe nazionale (comma 3). La disposizione disciplina altresì i flussi di dati che la Giunta può comunicare all'ufficio scolastico regionale, a quelli provinciali nonché ai comuni e ad altre istituzioni formative (agenzie formative accreditate e istituti professionali) (commi 6 e 7).

Premesso che il legislatore, disciplinando congiuntamente profili inerenti l'istruzione e la protezione dei dati personali, nell'ambito delle proprie competenze legislative esclusive, ha posto specifici vincoli alla residuale competenza legislativa regionale in materia (artt. 33, 117, secondo comma, lett. *l*), *m*), *n*), *r*), e terzo comma, Cost.), il Garante ha rilevato che le regioni possono costituire le proprie anagrafi regionali degli studenti nei limiti di quanto previsto dalla normativa nazionale (d.lgs. n. 76/2005) evitando la duplicazione di banche dati che possano contenere informazioni similari (d.l. 18 ottobre 2012, n. 179, convertito in l. 17 dicembre 2012, n. 221) e prevedendo la funzione di coordinamento del Ministero dell'istruzione, dell'università e della ricerca, da esercitarsi sentito il Garante (art. 13, d.l. 12 settembre 2013, n. 104, convertito dalla l. 8 novembre 2013, n. 128). In ogni caso le regioni possono effettuare il trattamento di dati personali nel rispetto dei presupposti e dei limiti stabiliti dal Codice (Corte cost. n. 271/2005), disciplina dettata dal legislatore nell'ambito della propria competenza esclusiva di cui all'art. 117, secondo comma, lett. *l*) ed *r*), Cost. Al riguardo, deve evidenziarsi, in particolare, che i soggetti pubblici possono trattare dati personali necessari, pertinenti e non eccedenti rispetto alle proprie specifiche funzioni istituzionali (artt. 3, 11, 18 del Codice).

Sulla base del predetto quadro normativo, si è ritenuto necessario segnalare alla Presidenza, per le conseguenti determinazioni, le seguenti criticità: 1) per quanto riguarda l'integrazione dell'anagrafe regionale con l'Ans (art. 14, comma 3), l'esigenza di assicurare il rispetto della funzione di coordinamento del Miur nell'integrazione e coordinamento delle banche dati del sistema nazionale delle anagrafi (art. 13, comma 2, d.l. n. 104/2013); 2) con riferimento ai dati contenuti nell'anagrafe regionale e ai flussi informativi (art. 14, commi 4, 6 e 7), il divieto di duplicazione di banche dati (in quanto alcune delle informazioni raccolte nella costituenda anagrafe regionale degli studenti sembravano essere già presenti nell'Ans, specie quelle relative al percorso scolastico: art. 10, comma 8, d.l. n. 179/2012) nonché il rispetto dei principi di pertinenza e non eccedenza delle informazioni raccolte nella predetta anagrafe e comunicate ad altri soggetti, anche mediante non meglio definiti "collegamenti" con i dati raccolti da altri settori (comma 4).

La legge regionale non è stata impugnata. Nondimeno la Regione Calabria ha valutato di integrare il comma 3 dell'art. 14 con il riferimento alla normativa nazionale segnalata dal Garante al fine di assicurare il rispetto delle funzioni di coordinamento del Ministero in tale materia, anche sotto il profilo della protezione dei dati personali (art. 1, l.r. 20 febbraio 2014, n. 5, in *Bur* 21 febbraio 2014, n. 8).

II - L'attività svolta dal Garante

4 Il Garante e le pubbliche amministrazioni

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

ADAMS

Dopo aver espresso parere favorevole rispetto al regolamento per il trattamento di dati sensibili e giudiziari adottato dal Comitato olimpico nazionale italiano (Coni) nel 2007 (provv. 19 settembre 2007, doc. web n. 1443411), il Garante è tornato ad esprimersi sul nuovo schema contenente talune modifiche e integrazioni motivate dalla necessità per il Coni di perseguire l'interesse pubblico sotteso alle attività di prevenzione e repressione del fenomeno del *doping* nello sport attraverso l'uso dell'*Anti-Doping Administration & Management System* (sistema ADAMS) (provv. 31 luglio 2014, n. 390, doc. web n. 3385186). Ciò nelle more della definizione, a livello europeo, di un quadro di garanzie unitario volto ad assicurare la conformità alla disciplina di protezione dei dati di alcuni aspetti della regolamentazione *anti-doping* fissata nel codice mondiale in materia e negli *standard* che lo completano (v. provv. 13 ottobre 2008, doc. web n. 1563970; pareri del Gruppo Art. 29 n. 3/2008 - WP 156, doc. web n. 1619614 e n. 4/2009 - WP 162, doc. web n. 1620339; lettere del Gruppo Art. 29 a WADA, doc. web nn. 2983092 e 2983102).

Come è noto, il sistema ADAMS, realizzato dall'Agenzia mondiale *anti-doping* (*World Anti-Doping Agency*-WADA), è costituito da una banca dati riferita agli atleti per pianificare e coordinare i controlli *anti-doping* situata in Canada (Québec). In particolare, sulla base delle regole fissate nel codice mondiale e nei relativi *standard*, sono registrati nella banca dati a cura degli stessi atleti, delle organizzazioni nazionali *anti-doping* e delle federazioni sportive di appartenenza dati identificativi e altre informazioni riferite all'atleta, quali i dati sui luoghi di reperibilità e permanenza (cd. *whereabouts*), sulle esenzioni a fini terapeutici, sulla pianificazione e distribuzione dei controlli *anti-doping* e sui singoli controlli effettuati.

Il parere è stato reso su una versione aggiornata dello schema tipo di regolamento all'esito di un proficuo lavoro di collaborazione con i competenti uffici del Coni, i quali, a seguito di numerose riunioni e contatti informali, hanno accolto le osservazioni formulate dall'Ufficio. Gli elementi forniti all'Autorità sono stati ritenuti idonei a garantire un adeguato quadro giuridico per i trattamenti di dati sensibili e giudiziari, effettuati dal Coni attraverso la banca dati ADAMS in quanto ente istituzionalmente preposto all'adozione e all'attuazione della normativa *anti-doping* (d.lgs. 23 luglio 1999, n. 242; Statuto del Coni; norme sportive *anti-doping*; artt. 18 ss. del Codice).

Tali trattamenti, che comportano flussi transfrontalieri di dati personali anche verso Paesi terzi (cfr. in merito anche par. 23.3) – limitati ai soli dati indispensabili ed effettuati mediante operazioni di trattamento non massive o ripetute –, risultano infatti necessari per il contrasto al *doping* e sono quindi riconducibili alle finalità di rilevante interesse pubblico individuate dal Codice, di applicazione della normativa in materia di sicurezza e salute della popolazione e di promozione dello sport (l. 14

dicembre 2000, n. 376; artt. 43, comma 1, lett. *c*), 73, comma 2, lett. *c*), e 85, comma 1, lett. *e*), del Codice). In particolare, i trattamenti di dati personali così effettuati dal Coni riguardano soltanto un gruppo selezionato di atleti (quelli inseriti nel *registered testing pool* nazionale), ferma restando la facoltà del Coni di disporre controlli anche su altri atleti. Con riferimento ai predetti atleti, il Coni potrà pertanto effettuare, ove necessario, operazioni di trasferimento all'estero di dati personali, anche sensibili e giudiziari, verso la banca dati ADAMS e verso le organizzazioni *anti-doping* ubicate anche in Paesi terzi di volta in volta competenti a testare gli atleti sulla base delle regole *dell'anti-doping*.

Altre indicazioni fornite dall'Ufficio, recepite dal Coni nel nuovo schema di regolamento, hanno riguardato le cautele previste a tutela dei diritti degli interessati nella pubblicazione sul sito istituzionale del Coni dei dati giudiziari contenuti nelle sentenze e negli altri provvedimenti adottati dagli organi di giustizia sportiva effettuati per finalità di comunicazione istituzionale e di informatica giuridica.

Regolamenti di dati sensibili e giudiziari

Sul tema dei regolamenti sul trattamento dei dati sensibili e giudiziari da parte di amministrazioni locali, l'Autorità è stata consultata dal Comune di Palermo prima dell'approvazione di un nuovo regolamento in sostituzione di quello previgente. In particolare, è stato richiesto se il nuovo regolamento potesse discostarsi dallo schema approvato con parere del Garante del 21 settembre 2005 e prevedere che l'identificazione e la pubblicazione dei tipi di dati e delle operazioni eseguibili potessero essere rinviate dal regolamento stesso ad un atto rimesso ai singoli settori, in ragione della competenza specialistica di ciascuno di essi. Al riguardo, l'Ufficio ha precisato che le amministrazioni non possono avvalersi di meri atti, i quali, anche quando (formalmente) denominati regolamenti, non hanno la necessaria natura di fonte normativa suscettibile di incidere su diritti e libertà fondamentali di terzi, dovendo assicurare l'emanazione dell'atto di natura regolamentare previsto dalla norma, anche promuovendone l'adozione da parte dell'organo competente in base all'ordinamento dell'amministrazione. La soluzione prospettata dal Comune, che intenderebbe rimettere ai singoli dirigenti dei settori l'adozione degli atti necessari a identificare e rendere pubblici i dati sensibili e le operazioni eseguibili, non è stata pertanto ritenuta conforme alle previsioni del Codice, con conseguente illeceità dei trattamenti di dati personali eventualmente effettuati su tali presupposti (note 11 aprile e 23 maggio 2014).

Unar

Con parere favorevole del 5 giugno 2014, n. 280 (doc. web n. 3248445), il Garante si è espresso sulle modifiche ed integrazioni apportate alla scheda n. 6 del regolamento per il trattamento di dati sensibili e giudiziari della Presidenza del Consiglio dei ministri relativa alla "Gestione degli interventi in ambito sociale, di pari opportunità e tutela dei soggetti vittime della discriminazione", effettuati dall'Ufficio nazionale antidiscriminazioni razziali (Unar) (d.P.C.M. 30 novembre 2006, n. 312).

La predetta scheda è stata modificata con l'aggiunta, nell'ambito della sezione relativa ai tipi di dati trattati, de "lo stato di salute: patologie attuali, patologie pregresse, terapie in corso anamnesi familiare"; e de "la vita sessuale". L'Unar ha rappresentato, sulla base del quadro normativo di seguito riportato, l'indispensabilità del trattamento dei predetti dati personali di natura sensibile in ragione del recente ampliamento dei compiti attribuiti all'Ufficio stesso (art. 22, comma 3, del Codice). In particolare, in base al d.P.C.M. 1° ottobre 2012, "il Dipartimento per le pari opportunità è la struttura di supporto al Presidente che opera nell'area funzionale inerente alla promozione ed al coordinamento delle politiche dei diritti della persona, delle pari opportunità e della parità di trattamento e delle azioni di Governo volte a prevenire e rimuovere ogni forma e causa di discriminazione" e "nell'ambito del

Dipartimento opera altresì l'Ufficio per la promozione delle parità di trattamento e la rimozione delle discriminazioni fondate sulla razza e sull'origine etnica di cui all'art. 29 della legge 1° marzo 2002, n. 39" (art. 16, commi 1 e 5).

Anche il successivo d.m. 4 dicembre 2012 ha ampliato i compiti affidati all'Unar, attribuendogli la funzione di garantire l'effettività del principio di parità di trattamento tra le persone e di vigilare sull'operatività degli strumenti di tutela vigenti contro le discriminazioni fondate su tutti i fattori di comportamenti discriminatori con particolare riferimento a quelle derivanti dalla razza e dall'origine etnica (art. 8, comma 1). A tal fine, il Servizio per la tutela della parità di trattamento presso l'Unar si occupa, in particolare, di gestire la raccolta delle segnalazioni in ordine a casi di discriminazione.

4.2. *Le grandi banche dati pubbliche*

Inps

Lo schema di convenzione redatto dall'Inps ai sensi dell'art. 58, comma 2, del Cad, per la fruibilità telematica delle proprie banche dati ha formato oggetto di esame da parte del Garante. La richiamata disposizione 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. Sul tema, l'Autorità è già intervenuta nel 2013 con un parere favorevole reso all'Agenzia per l'Italia Digitale (AgID) riguardante le "Linee guida per la stesura di convenzioni per la fruibilità di dati delle pubbliche amministrazioni" (v. provv. 4 luglio 2013, n. 332, doc. web n. 2574977; v. anche Relazione 2013, p. 36). Il richiamato quadro normativo di settore disciplinato dall'art. 58, c. 2, del Cad, è stato modificato dalla legge 11 agosto 2014, n. 114: con l'innovazione introdotta si prevede che le pubbliche amministrazioni comunichino tra loro attraverso la messa a disposizione a titolo gratuito degli accessi alle proprie basi di dati alle altre amministrazioni mediante la cooperazione applicativa di cui all'art. 72, comma 1, lett. *e*). L'AgID, sentiti il Garante e le amministrazioni interessate alla comunicazione telematica, è chiamata a definire gli *standard* di comunicazione e le regole tecniche a cui le pubbliche amministrazioni devono conformarsi.

In ragione della rilevanza dei dati, anche sensibili, trattati presso i sistemi informativi dell'Inps e dell'ingente numero di soggetti legittimati ad accedervi, si è esaminato lo schema di convenzione quadro predisposto dell'Inps sulla base delle predette "Linee guida" al fine di verificare la necessità di individuare ulteriori misure e accorgimenti. Lo schema, elaborato dall'Istituto alla luce degli approfondimenti svolti in collaborazione con l'Ufficio, anche nel corso di accertamenti ispettivi, riguarda soltanto gli accessi delle pp.aa. e dei gestori di pubblico servizio per finalità di controllo delle autocertificazioni e per finalità istituzionali e non fa riferimento agli accessi da parte di intermediari, caf e patronati. Il documento ha ottenuto il parere favorevole del Garante in considerazione delle specifiche misure e degli accorgimenti, anche di carattere organizzativo, ivi previsti, ritenuti idonei a ridurre al minimo i rischi per la sicurezza dei dati, tenuto conto delle particolari caratteristiche dei trattamenti effettuati presso l'Istituto (provv. 6 marzo 2014, n. 108, doc. web n. 3033479).

A seguito dei numerosi casi di accessi abusivi ai sistemi informativi dell'Inps (v. già Relazione 2013, p. 38), in relazione ai quali sono in corso ulteriori verifiche da parte dell'Istituto, l'Ufficio ha segnalato l'esigenza di approntare opportune misure tecniche e organizzative per bloccare tempestivamente eventuali accessi impropri e per prevenire il rischio che tali illeciti si ripetano (note 27 maggio e 28 agosto 2014).

Al riguardo, merita segnalare che, nell'ambito degli approfondimenti ispettivi riguardanti l'accesso dall'esterno alle banche dati dell'Inps, l'Istituto ha comunicato all'Autorità di aver intrapreso un processo di ridefinizione delle misure di sicurezza riguardanti l'accesso ai propri sistemi informativi da parte di soggetti esterni abilitati (professionisti, caf e patronati). Sulla base delle risultanze emerse nel corso di tali approfondimenti e delle interlocuzioni intercorse con l'Ufficio, le misure predisposte prevedono, in particolare, la digitalizzazione e la trasmissione telematica da parte degli intermediari di copia del documento di riconoscimento dell'interessato e del mandato da questi conferito all'intermediario al fine di prevenire i rischi di accessi indebiti volti al rilascio delle certificazioni unificate dei redditi di lavoro dipendente, equiparati e assimilati (cud). L'Inps ha altresì comunicato di aver avviato la messa a punto di un nuovo sistema di controllo e di *audit* finalizzato a verificare la regolarità degli accessi alle proprie banche dati da parte di intermediari esterni; in particolare, l'Istituto intende introdurre un sistema di blocco automatico preventivo degli accessi anomali (per contrastare il *download* massivo di dati contributivi tramite procedure robotizzate e i casi di ripetute visualizzazioni di cud da parte di diversi operatori), nonché implementare un sistema di monitoraggio a posteriori degli accessi al fine di verificare la sussistenza presso l'intermediario del documento di riconoscimento dell'interessato e del mandato dallo stesso conferito. Tali misure, in corso di definizione in seno all'Inps, saranno portate a conoscenza dell'Autorità per le valutazioni di competenza.

Spid

Come riferito (par. 3.4.1), il Garante ha reso parere su uno schema di decreto del Presidente del Consiglio dei ministri recante la definizione delle caratteristiche del "Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese" (Spid) nonché dei tempi e delle modalità di adozione del sistema da parte delle pubbliche amministrazioni e delle imprese, adottato ai sensi dell'articolo 64 del Cad (parere 19 giugno 2014, n. 311, doc. web n. 3265492). Il decreto esaminato è un primo provvedimento adottato in materia, le cui disposizioni, anche per i profili di protezione dei dati, rinviano a successivi atti che dovranno essere adottati dall'Agenzia per l'Italia digitale (AgID), previo parere dell'Autorità, e in cui saranno specificate le regole tecniche e le modalità attuative per la realizzazione dello Spid, le modalità di accreditamento dei soggetti coinvolti, le procedure per il rilascio dell'identità digitale, nonché le convenzioni sulla verifica e l'uso dei dati.

L'identità digitale è l'insieme degli attributi identificativi della persona, fisica o giuridica, raccolti e registrati in forma digitale. In sostanza si tratta di un codice identificativo univoco dotato di attributi identificativi obbligatori (codice fiscale, nome, cognome, comune di nascita, sesso) nonché di attributi secondari, quali la casella Pec, il numero di telefono fisso o mobile e di attributi qualificati (ad es. la qualifica professionale). Infine a ogni identità è associata una credenziale per accedere, tramite autenticazione informatica, ai servizi erogati in rete.

L'identità digitale è rilasciata dai "gestori dell'identità digitale", persone giuridiche che devono accreditarsi presso l'AgID e sono iscritti nel registro pubblico Spid. I gestori conservano, rendono disponibili e gestiscono gli attributi e le credenziali di autenticazione utilizzati dall'utente per l'accesso ai servizi. Il rilascio dell'identità digitale presuppone la verifica dell'identità del richiedente che può avvenire attraverso un contatto diretto (unico livello di verifica mantenuto per garantire un alto livello di sicurezza, anche se non in linea con altri progetti europei). Tale verifica può essere effettuata in diversi modi. Il riconoscimento *de visu* non è però sempre richiesto: se il richiedente possiede già un documento digitale di identità (CIE, CNS, TS-CNS) l'identità Spid potrà essere rilasciata senza ripetere la verifica, con una semplice richiesta *online*.

Oltre ai gestori di identità, sono coinvolti nel Sistema i "gestori di attributi qualificati" – ovvero soggetti che per legge sono titolati a certificare alcuni attributi qualificanti, come ad esempio un'abilitazione professionale, anch'essi accreditati presso l'AgID – e i "fornitori dei servizi", soggetti pubblici o privati che sottoscrivono apposite convenzioni con AgID e che erogano servizi via internet per i quali sia richiesta l'identificazione e l'autenticazione degli utenti. Tutti questi soggetti sono iscritti nel registro Spid.

Nel suo complesso, il Sistema è volto a favorire la diffusione di servizi in rete e ad agevolare l'accesso agli stessi mediante l'attribuzione a ciascun soggetto interessato di un'"identità digitale" allo scopo di identificare in modo univoco chi si rivolge, ad esempio, alla pubblica amministrazione per richiedere il servizio (come il rilascio di un certificato). L'istituzione di un sistema pubblico di identità dovrebbe consentire di disporre di identità digitali "sicure", in grado cioè di minimizzare anche i rischi di crimini informatici come il furto d'identità.

Il Garante ha espresso parere favorevole sullo schema di decreto, subordinandolo però al recepimento di numerose condizioni volte a perfezionare il testo e a renderlo conforme alla disciplina in materia di protezione dei dati personali.

L'architettura del sistema – anche se soggetto a conferma nei documenti attuativi – dovrebbe consentire ai cittadini di rivolgersi a vari gestori di identità e di dotarsi di più strumenti di identificazione, da utilizzare a seconda dei diversi contesti, anche tenendo conto del livello di sicurezza di volta in volta richiesto.

Il Sistema dovrebbe lasciare in vita la possibilità di utilizzare, per l'accesso ai servizi, anche la carta d'identità elettronica e la carta nazionale dei servizi. Tuttavia, mentre queste ultime presuppongono che i dati necessari per verificare l'identità in rete siano tutti disponibili al soggetto che offre il servizio, con Spid dovrebbero essere forniti a quest'ultimo solo i dati strettamente necessari per lo specifico servizio reso: ad esempio, se è necessario sapere unicamente che il richiedente è maggiorenne, potrà essere fornita solo tale informazione e non anche l'indirizzo di residenza o la data di nascita.

Inoltre, la presenza di più gestori di identità evita i rischi connessi alla creazione di una banca dati centralizzata delle identità, scongiurando che il sempre possibile suo malfunzionamento o violazione della stessa porti al crollo dell'intero sistema o a danni gravissimi per gli interessati.

Naturalmente, tutti questi aspetti, che astrattamente dovrebbero essere positivi dal punto di vista della protezione dei dati personali, dovranno essere verificati, attraverso l'esame degli atti applicativi, in sede di parere del Garante, oltre che nel funzionamento in concreto del Sistema.

Casellario dell'assistenza

Come anticipato (par. 3.4.1), l'Autorità si è altresì occupata dell'anagrafe generale delle posizioni assistenziali costituita presso l'Inps come partizione del Sistema informativo dei servizi sociali di cui all'art. 21, l. 8 novembre 2000, n. 328 (di seguito Siss) che raccoglie informazioni sulle prestazioni sociali erogate, sulle caratteristiche personali e familiari nonché sulla valutazione del bisogno dei beneficiari di tali prestazioni (cd. Casellario dell'assistenza: provv. 23 gennaio 2014, n. 26, doc. web n. 2922956). Si è così inteso assicurare una compiuta conoscenza dei bisogni sociali e consentire il monitoraggio della spesa e la programmazione, la valutazione dell'efficienza e dell'efficacia degli interventi nonché l'elaborazione di statistiche e la conduzione di studi e di ricerche nel settore dell'assistenza sociale. A questo scopo, le amministrazioni locali e ogni altro ente che eroga tali prestazioni devono mettere a disposizione del Casellario le informazioni previste dal decreto – quali i dati riguardanti le caratteristiche socio-demografiche e familiari dei beneficiari, nonché le informazioni sugli enti eroganti e sulle prestazioni erogate – e l'Inps deve renderle

disponibili in forma individuale, ma prive di ogni riferimento che ne permetta il collegamento con gli interessati o li renda comunque identificabili, al Ministero del lavoro, al Ministero dell'economia e delle finanze, alle Regioni, alle Province autonome e ai Comuni.

Inoltre, nel caso in cui all'erogazione della prestazione sia associata la presa in carico da parte del servizio sociale, è previsto che in apposite sezioni separate, dedicate alle persone non autosufficienti, in condizioni di povertà e ai minori in condizioni di disagio siano raccolte anche informazioni sulla valutazione del bisogno sociale. I dati direttamente identificativi dei beneficiari sono consultabili dagli enti locali con riferimento alle prestazioni da essi erogate e a quelle erogate dall'Inps. Garanzie ulteriori, volte a prevenire l'identificabilità degli interessati, sono previste per le informazioni contenute nella sezione dedicata ai minori in condizioni disagio. Hanno infine accesso alla banca dati la Guardia di finanza e l'Agenzia delle entrate per effettuare controlli sui beneficiari delle prestazioni.

Nello schema di decreto sottoposto all'Autorità, che ha recepito le indicazioni suggerite dall'Ufficio al Ministero del lavoro nel corso di riunioni e contatti informali, sono state circoscritte le tipologie di prestazioni sociali destinate a confluire nel Casellario prevedendo, in particolare, che questo raccolga informazioni connesse alle sole prestazioni sociali per la cui erogazione è necessaria l'identificazione del beneficiario. In considerazione dell'estrema delicatezza dei dati trattati e della vulnerabilità degli interessati, sono state inoltre definite le modalità di aggregazione e di anonimizzazione delle informazioni relative ai minori in situazione di disagio. Infine, l'Ufficio è intervenuto nella delimitazione dei soggetti legittimati ad accedere al Casellario e nella specificazione dei presupposti, finalità e modalità di accesso. Le modalità attuative e le specifiche tecniche per la raccolta, la trasmissione, lo scambio e l'anonimizzazione dei dati, nonché le misure di sicurezza del Casellario saranno definite dall'Inps con successivi decreti, sentito il parere del Garante.

Dsu

Parere favorevole è stato espresso sullo schema di provvedimento del Ministero del lavoro e delle politiche sociali di approvazione del modello tipo di dichiarazione sostitutiva unica (Dsu) per il calcolo dell'Indicatore della situazione economica equivalente (Isee), ai sensi dell'art. 10, comma 3, d.P.C.M. 5 dicembre 2013, n. 159 (provv. 6 novembre 2014, n. 495, doc. web 3515450). Come è noto, il citato d.P.C.M. n. 159/2013 – recante il regolamento concernente la revisione delle modalità di determinazione e i campi di applicazione dell'Isee, sul cui schema il Garante aveva fornito il parere di competenza (22 novembre 2012, n. 361, doc. web n. 2174496) – prevede che l'Isee venga calcolato sulla base delle informazioni, relative al nucleo familiare di appartenenza del beneficiario, fornite dal dichiarante attraverso un apposito modello di dichiarazione ("dichiarazione sostitutiva unica" – Dsu) nonché delle altre informazioni disponibili negli archivi dell'Inps e dell'Agenzia delle entrate, acquisite dal sistema informativo dell'Isee (artt. 2, comma 6, e 11).

Ciò premesso, il parere in esame è stato reso su una versione di modello di Dsu che tiene conto degli approfondimenti e delle indicazioni suggerite dall'Ufficio, anche nel corso di riunioni di lavoro e contatti informali, al competente ufficio del Ministero volti a perfezionare il testo e a renderlo conforme alla disciplina in materia di protezione dei dati personali, in relazione alle operazioni di raccolta delle informazioni relative al nucleo familiare di appartenenza del beneficiario di una prestazione sociale, nonché di consegna da parte degli enti legittimati dell'attestazione dell'Isee, del contenuto della Dsu e di eventuali ulteriori informazioni comunque necessarie al calcolo dell'Isee. Su tali basi, in particolare, l'informativa è stata formalmente inserita nella parte iniziale del modello. Inoltre, è stato precisato che le informazioni indicate nella Dsu come facoltative perseguono finalità di

accesso a determinate prestazioni sociali ovvero di contatto con il dichiarante. Infine, è stato evidenziato all'interno dell'informativa che i controlli sulle informazioni rese dal dichiarante avranno ad oggetto anche i dati personali dei componenti il nucleo familiare. Con riferimento alle modalità per rendere le Dsu disponibili ai dichiaranti è stato specificato che questi ultimi possono eventualmente conferire mandato ai soggetti incaricati della ricezione della Dsu (centri di assistenza fiscale o enti erogatori) a ricevere, ai soli fini del rilascio ai dichiaranti stessi, l'attestazione contenente l'Isee e le altre informazioni usate per il calcolo e, in tal caso, richiedere contestualmente all'Inps di rendere disponibili le medesime informazioni e attestazioni.

Il parere del 12 giugno 2014, n. 295 (doc. web n. 3255963) è invece dedicato al sistema informativo nazionale per la prevenzione nei luoghi di lavoro (Sinp), articolato sistema informativo istituito presso l'Inail (ora Inps) che coinvolge più archivi informativi riferibili a diversi soggetti istituzionali contenente, tra l'altro, dati sensibili dei lavoratori (cfr. par. 3.4.1).

Sinp

4.3. *L'accesso ai documenti amministrativi*

L'Autorità è frequentemente chiamata ad intervenire sulle tematiche riguardanti l'accesso ai documenti amministrativi (sovente a seguito del mancato riscontro, oppure del diniego di accesso opposto dalle amministrazioni, non di rado adducendo generici rinvii alla disciplina in materia di protezione dei dati personali) e sulla presunta violazione di norme sul relativo procedimento amministrativo. In tali occasioni l'Ufficio ha ribadito che il Codice non ha abrogato le norme vigenti in materia di accesso ai documenti amministrativi (artt. 59 e 60 del Codice), le quali attribuiscono il diritto di prendere visione e di estrarre copia di documenti amministrativi ai soggetti che abbiano un interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso (artt. 22 e ss., l. 7 agosto 1990, n. 241, così come modificata dalla l. 11 febbraio 2005, n. 15; art. 2, d.P.R. 12 aprile 2006, n. 184). In questi casi, infatti, spetta all'amministrazione destinataria dell'istanza entrare nel merito ed accertare l'eventuale qualificata posizione di pretesa all'informazione del richiedente. Inoltre, le valutazioni in ordine alle determinazioni assunte sull'accesso esulano dall'ambito di competenza di questa Autorità e rimangono sindacabili di fronte alle autorità competenti (art. 25, l. n. 241/1990, come modificata dalla l. n. 15/2005) (note 2 e 17 settembre 2014 nonché 19 novembre 2014).

In tale contesto, appare utile evidenziare una segnalazione relativa alla produzione, in allegato a una denuncia, di atti e documenti contenenti dati personali asseritamente acquisiti in modo illecito presso un comune; pur non essendo stata accertata l'acquisizione degli atti in violazione dei presupposti di legittimità previsti dalla legge, l'Ufficio ha ricordato che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali eventualmente non conforme a disposizioni di legge o di regolamento, restano comunque disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale e che spetta al giudice, ove ritualmente richiesto, valutare la liceità del trattamento dei dati personali dell'interessato (art. 160, comma 6, del Codice) (nota 25 novembre 2014).

Su richiesta del Ministero delle politiche agricole, alimentari e forestali, l'Autorità è stata inoltre chiamata ad esprimere le proprie valutazioni in ordine ai rapporti tra l'accesso difensivo ai sensi dell'art. 24, comma 7, l. 7 agosto 1990, n. 241 e le dispo-

sizioni preclusive previste dagli artt. 2, 3 e 4, d.m. 5 settembre 1997, n. 392, che individua le categorie di atti sottratti all'accesso presso il predetto Ministero. In proposito, è stato evidenziato che su tali questioni il Garante ha adottato un provvedimento di carattere generale (cfr. provv. 9 luglio 2003, doc. web n. 29832) sui diritti di cd. pari rango nel quale si forniscono specifiche indicazioni sulla valutazione che le amministrazioni sono tenute ad effettuare in relazione ai diversi diritti in gioco (nota 5 marzo 2014).

Vitalizi

La Regione Lombardia ha interpellato l'Autorità in ordine alla possibilità di pubblicare sul sito istituzionale i nominativi dei consiglieri percettori di assegno vitalizio, con specificazione degli importi, della decorrenza e del complessivo ammontare dei contributi versati, nonché di rilasciare tale documentazione ad un giornalista che l'aveva richiesta, ai sensi della l. n. 241/1990, unitamente all'elenco dei consiglieri della trascorsa legislatura che avevano optato per il riscatto dei contributi e di quelli che avevano optato per i vitalizi. L'Ufficio, nel ribadire la piena vigenza delle norme in materia di accesso ai documenti amministrativi (artt. 59 e 60), ha evidenziato che tali disposizioni, non avendo inciso in modo restrittivo sulla normativa posta a salvaguardia della trasparenza amministrativa, non possono essere invocate per negare, in via di principio, l'accesso ai documenti. Inoltre, nel caso in cui l'Amministrazione reputi legittima la richiesta di accesso, rimane "affidata alla responsabilità del giornalista l'utilizzazione lecita del dato raccolto e quindi la sua diffusione secondo i parametri dell'essenzialità rispetto al fatto d'interesse pubblico narrato, della correttezza, della pertinenza e della non eccedenza, avuto altresì riguardo alla natura del dato medesimo" (cfr. nota 6 maggio 2004, doc. web n. 1007634). Tale precisazione, rivolta a chi utilizza la documentazione a cui ha avuto legittimamente accesso per l'esercizio dell'attività giornalistica, costituisce un'applicazione dei principi generali dettati dal Codice per i trattamenti svolti in ambito giornalistico (cfr. art. 137 e All. A.1 al Codice) (nota 3 febbraio 2014).

Accesso dei consiglieri comunali

Sono state sottoposte all'attenzione del Garante anche numerose problematiche riguardanti l'accesso di consiglieri comunali agli atti degli enti locali di appartenenza.

Al quesito sulla legittimità di consentire l'accesso al protocollo mediante l'estrazione di copia dei documenti riferiti al singolo numero di protocollo attraverso apposita richiesta scritta, oppure se fosse legittimo consentire la consultazione diretta del predetto registro mediante il rilascio di apposite credenziali di accesso, l'Ufficio, oltre a richiamare la giurisprudenza amministrativa sul punto ed i provvedimenti di carattere generale già emanati (cfr., tra gli altri, nota 20 maggio 1998, doc. web n. 40979; comunicato stampa 9 giugno 1998, doc. web n. 48924; parere 10 giugno 1998, doc. web n. 39348; nota 8 giugno 1999, doc. web n. 40369; nota 8 febbraio 2001, doc. web n. 1075036; nota 4 aprile 2001, doc. web n. 42070; provv. 14 luglio 2005, doc. web n. 1157675, e da ultimo provv. 25 luglio 2013, n. 369, doc. web n. 2604062), ha evidenziato la piena vigenza della norma 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). Quanto all'individuazione delle notizie e informazioni utili alle quali può essere consentito l'accesso, deve farsi riferimento a tutti gli atti che possano essere effettivamente utili allo svolgimento dei compiti del consigliere e alla sua partecipazione alla vita politico-amministrativa dell'ente. Ciò al fine di permettere di valutare, con piena cognizione, la correttezza e l'efficacia dell'operato dell'amministrazione nonché per esprimere un voto consapevole sulle questioni di competenza del Consiglio e per promuovere le iniziative che spettano ai singoli rappresentanti del corpo elettorale locale (cfr., ad es., C.d.S., Sez. V, 17 settem-

bre 2010, n. 6963). Spetta, pertanto, all'Amministrazione entrare nel merito della valutazione della richiesta ed accertare l'ampia e qualificata posizione di pretesa all'informazione *ratione officii* del consigliere comunale, valutazione eventualmente sindacabile dal giudice amministrativo. La finalizzazione dell'accesso all'espletamento del mandato costituisce il presupposto che legittima l'accesso e che, al tempo stesso, ne delimita la portata (nota 3 aprile 2014).

Altre fattispecie hanno riguardato eventuali limiti all'accesso dei consiglieri comunali laddove le informazioni contenute nella documentazione rivestano particolare delicatezza, come nel caso di una richiesta concernente l'accesso alla relazione integrale dell'assistente sociale contenente dati sensibili, oppure a documentazione contenuta nel fascicolo relativo ad un minore in carico ai servizi sociali del comune, contenente dati sensibili riferiti allo stesso. Al riguardo è stato evidenziato che, nell'ipotesi in cui l'accesso dei consiglieri comunali riguardi dati sensibili, l'esercizio di tale diritto, ai sensi dell'art. 65, comma 4, lett. *b*), del Codice, è consentito in quanto indispensabile allo svolgimento della funzione di controllo, di indirizzo politico, di sindacato ispettivo e di altre forme di accesso a documenti riconosciute dalla legge e dai regolamenti degli organi interessati per consentire l'espletamento di un mandato elettivo (v. scheda n. 33 dello schema tipo Anci, doc. web n. 1174532, sul quale l'Autorità si è espressa positivamente con parere del 21 settembre 2005, doc. web n. 1170239; cfr. anche provv. 25 luglio 2013, n. 369, doc. web n. 2604062). I dati personali eventualmente acquisiti devono essere utilizzati effettivamente per le sole finalità realmente pertinenti al mandato, rispettando l'obbligo del segreto "nei casi specificamente determinati dalla legge" nonché i divieti di divulgazione dei dati personali (ad es. art. 22, comma 8, del Codice che vieta la diffusione dei dati idonei a rivelare lo stato di salute) (note 12 marzo e 4 settembre 2014).

4.4. *La trasparenza amministrativa*

Per quanto riguarda il tema della trasparenza e della pubblicazione in internet di dati personali, a seguito dell'entrata in vigore del d.lgs. n. 33/2013 e considerate le numerose istanze ricevute, il Garante ha adottato le "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" (provv. 15 maggio 2014, n. 243, doc. web n. 3134436: in merito v. pure par. 13.3).

Le nuove Linee guida sono state elaborate tenuto conto delle osservazioni e dei riscontri ricevuti dal Dipartimento della funzione pubblica, dall'Autorità nazionale anticorruzione e per la valutazione e la trasparenza delle amministrazioni pubbliche (già Civit e ora Anac) e dall'AgID ed hanno sostituito le precedenti "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).

Il Garante ha, in primo luogo, sottolineato che rimane ferma la regola generale per la quale i soggetti pubblici possono diffondere dati personali solo se ciò è ammesso da una specifica disposizione di legge o di regolamento (art. 19, comma 3, del Codice).

In tal quadro, è necessario distinguere fra obblighi di pubblicazione *online* di dati per finalità di trasparenza oppure per altre finalità della p.a. (ad es., albo pretorio o altre forme di pubblicità dichiarativa, notizia o integrativa dell'efficacia) cui si applicano le indicazioni contenute, rispettivamente, nella prima e nella seconda parte delle Linee guida.

Anche in presenza di un obbligo di pubblicazione *online* le pp.aa. devono comunque selezionare i dati personali da inserire negli atti e documenti oggetto di pubblicazione e verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni nel rispetto del principio di pertinenza e non eccedenza dei dati personali nonché, nel caso dei dati sensibili, di indispensabilità.

Restano fermi alcuni divieti di diffusione di dati personali. In particolare, è sempre vietato diffondere dati idonei a rivelare lo stato di salute – ossia qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici – nonché dati idonei a rivelare la vita sessuale quando la pubblicazione è effettuata per finalità di trasparenza (art. 4, comma 6, d.lgs. n. 33/2013).

L'indicizzazione dei dati nei motori di ricerca generalisti (ad es., Google) durante il periodo di pubblicazione obbligatoria è limitato ai soli dati tassativamente individuati dalle norme in materia di trasparenza. Vanno quindi esclusi gli altri dati che si ha l'obbligo di pubblicare per altre finalità di pubblicità (ad es., pubblicità legale sull'albo pretorio, pubblicazioni matrimoniali, ecc.).

Il Garante ha inoltre precisato che in ogni caso i dati pubblicati *online* non sono liberamente riutilizzabili da chiunque per qualunque finalità, poiché l'obbligo previsto dalla normativa in materia di trasparenza *online* della p.a. di pubblicare dati in "formato aperto" non comporta che tali dati siano anche "dati aperti", cioè liberamente utilizzabili da chiunque per qualunque scopo. Al fine di chiarire tale circostanza, le amministrazioni sono invitate a inserire nella sezione denominata "Amministrazione trasparente" dei propri siti web un *alert* con cui si informa il pubblico che i dati personali sono "riutilizzabili solo alle condizioni previste dalla normativa vigente sul riuso dei dati pubblici (direttiva 2003/98/CE e d.lgs. n. 36/2006 di recepimento della stessa), in termini compatibili con gli scopi per i quali sono stati raccolti e registrati, e nel rispetto della normativa in materia di protezione dei dati personali".

È stato oltresì precisato che il periodo di mantenimento di dati, informazioni e documenti sul web coincide in linea di massima con il termine di cinque anni, ma anche che laddove atti, documenti e informazioni oggetto di pubblicazione obbligatoria per finalità di trasparenza contengano dati personali, questi ultimi devono essere oscurati, anche prima del termine di cinque anni, quando sono stati raggiunti gli scopi per i quali sono stati resi pubblici e gli atti stessi hanno prodotto i loro effetti.

Nel caso di pubblicazione di atti e documenti, per finalità diverse da quelle di trasparenza, rimangono invece ferme le specifiche disposizioni di settore (ad es., quindici giorni per la pubblicazione delle deliberazioni all'albo pretorio degli enti locali ai sensi dell'art. 124, d.lgs. 18 agosto 2000, n. 267). Se, invece, la disciplina di settore non stabilisce un limite temporale alla pubblicazione degli atti, vanno individuati – a cura delle amministrazioni titolari del trattamento – congrui periodi di tempo entro i quali mantenerli *online*, ma questo lasso di tempo non può essere superiore al periodo ritenuto, caso per caso, necessario al raggiungimento degli scopi per i quali i dati personali stessi sono resi pubblici.

Anche alla luce di tali indicazioni il Garante è intervenuto in numerose questioni sottoposte alla propria attenzione di cui si riportano le più rilevanti.

Con riferimento alla diffusione di dati personali *online* in assenza di idonei presupposti normativi, è stata riscontrata una condotta non conforme alla disciplina applicabile in ordine ai dati personali contenuti in numerosi documenti pubblicati sui siti web istituzionali come, fra gli altri, i verbali della commissione elettorale comunale relativi alla revisione e all'aggiornamento dell'albo unico degli scrutatori

di seggio elettorale (con indicazione dei nominativi degli interessati, luogo e data di nascita, indirizzo, motivo della non inclusione o della cancellazione nell'albo degli scrutatori oppure notizia della relativa iscrizione) (nota 22 agosto 2014); i provvedimenti amministrativi di cancellazione anagrafica per irreperibilità (nota 4 dicembre 2014); le fotocopie di carte di identità o di patenti di guida (nota 8 gennaio 2014); i nomi degli utenti morosi che utilizzano il servizio *pre* e *post* scuola con indicazione del nome del bambino, quello del genitore, numero di cellulare, indirizzo dell'abitazione, scuola frequentata dal minore e la somma ancora non pagata per il servizio (nota 4 dicembre 2014); la copia degli atti da notificare e contestazioni di sanzioni amministrative (con indicazione in chiaro dei dati personali del destinatario del provvedimento) (nota 29 settembre 2014); le immagini in chiaro dei bambini in costume da bagno ammessi alla colonia estiva del comune (nota 19 agosto 2014); le deliberazioni pubblicate sull'albo pretorio degli enti locali per più di quindici giorni (nota 8 ottobre 2014).

Dati sanitari

Con riferimento alla diffusione di dati personali *online* idonei a rivelare lo stato di salute, il Garante è intervenuto nei confronti di un'azienda sanitaria che ha pubblicato in internet le delibere relative alla liquidazione di fatture per l'inserimento di un minore in una comunità terapeutica riabilitativa. A tali delibere erano state allegate le copie integrali delle fatture relative alla retta della comunità che contenevano in chiaro e per esteso i dati anagrafici del giovane (nome, cognome, data e luogo di nascita) causando una diffusione di dati sul suo stato di salute vietata dalle norme in materia di protezione dei dati personali (provv. 6 novembre 2014, n. 494, non pubblicato ai sensi dell'art. 24 del Regolamento del Garante del 1° agosto 2013). Sullo stesso tema, è stata riscontrata una condotta non conforme alla disciplina applicabile in ordine alla pubblicazione sul sito web istituzionale di determinazioni aventi a oggetto "il ricovero urgente in ospedale di persona affetta da malattia mentale" (Tso) con indicazione in chiaro dei dati dell'interessato e della relativa patologia (nota 22 agosto 2014), oppure la concessione dei benefici di cui all'art. 33, comma 3, l. n. 104/92 con espliciti riferimenti alla condizione di handicap della figlia di un dipendente avente diritto al predetto beneficio (nota 22 agosto 2014).

Dati giudiziari

È stata altresì stigmatizzata la pubblicazione sul sito web istituzionale di un comune del decreto del Ministro dell'interno di rigetto della domanda di cittadinanza contenente dati personali anche giudiziari dell'interessato (nota 14 gennaio 2014) ed è stato chiarito, a un comune che aveva intenzione di pubblicare sul sito internet istituzionale il certificato del casellario giudiziale del sindaco, degli assessori e dei membri di "maggioranza" dei componenti il consiglio comunale, che il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (art. 21, comma 1) (nota 22 agosto 2014).

Sempre in tema di trasparenza, il Garante è stato poi interpellato con riferimento alla questione della reperibilità in rete, tramite i motori di ricerca generalisti (es. Google), di dati personali anche sensibili e giudiziari contenuti negli atti pubblicati sul sito web istituzionale della Camera dei deputati, nonché sul profilo della conoscibilità dei documenti formati e acquisiti dalle Commissioni parlamentari di inchiesta.

In ordine alla prima questione, confermando i precedenti orientamenti in materia (cfr. Relazione 2012, p. 70), è stato fatto presente che i lavori delle istituzioni parlamentari sono soggetti a regime di pubblicità (artt. 65 e 144 del regolamento della Camera e 33 del regolamento del Senato) e che i principi inerenti al trattamento dei dati sensibili e giudiziari sono applicabili ai trattamenti svolti dalla Presidenza della

Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte Costituzionale "in conformità ai rispettivi ordinamenti" (art. 22, comma 12, del Codice). È stato altresì ricordato che l'Ufficio di Presidenza della Camera dei deputati, con la delibera n. 46 del 2013, come modificata dalla delibera n. 53 del 2013, ha adottato una disciplina concernente la "Procedura in ordine a richieste concernenti dati personali contenuti in atti parlamentari" (disponibile in *www.camera.it/leg17/672?conoscerelacamera=316*) relativa alle modalità con cui i cittadini possono fare istanza direttamente alla Presidenza della Camera dei deputati con riferimento "a loro dati personali contenuti in atti parlamentari pubblicati sul sito internet della Camera dei deputati" (nota 5 giugno 2014).

In relazione, invece, alla pubblicazione sul sito istituzionale di atti e documenti delle Commissioni parlamentari d'inchiesta è stato rappresentato che esistono due diverse tipologie di atti e documenti: quelli "formati" dalla Commissione d'inchiesta stessa (come i resoconti delle audizioni) e quelli, invece, solo "acquisiti" dalla Commissione stessa in quanto prodotti da soggetti esterni.

Fino a oggi, tale tipologia di atti e documenti formati o acquisiti dalle Commissioni parlamentati d'inchiesta è stata soggetta a un preciso regime di pubblicità, differenziato in ragione della "diversa natura dei documenti in esame", che prevede la pubblicazione sul sito web istituzionale della Camera degli atti formati dalle Commissioni, in quanto soggetti al principio di pubblicità dei lavori parlamentari ai sensi dell'art. 64 Cost., e la mera consultabilità, presso i locali dell'archivio storico dei documenti acquisiti dalla Commissione nel corso dell'inchiesta da parte di chiunque ne faccia richiesta.

Con riferimento all'interesse alla conoscibilità dei documenti "acquisiti" dalle Commissioni d'inchiesta, occorre tenere conto che gli stessi sono stati oggetto del vaglio della Commissione e le informazioni ritenute di interesse ai fini dell'inchiesta sono state presumibilmente evidenziate nelle relazioni – di maggioranza ed, eventualmente, di minoranza – già integralmente pubblicate. Di conseguenza, le eventuali ulteriori informazioni che emergano dai documenti esterni acquisiti dalla Commissione – e che giustifichino la successiva ostensione dei documenti medesimi – potrebbero essere state ritenute dai diversi componenti della Commissione irrilevanti o addirittura inattendibili.

Considerata quindi la notevole varietà del contenuto e dei dati personali, anche sensibili e giudiziari, inseriti soprattutto negli atti esterni acquisiti dalle Commissioni parlamentari d'inchiesta per l'esercizio delle proprie funzioni, spetta ai competenti organi della Camera – alla luce dei principi in materia di protezione dei dati personali prima richiamati – effettuare il più corretto bilanciamento fra l'interesse alla piena conoscibilità della documentazione dell'attività delle menzionate Commissioni e la riservatezza delle informazioni in essa contenute.

In ogni caso, tenendo conto della "diversa natura dei documenti in esame", l'Ufficio ha ritenuto che gli organi della Camera hanno correttamente differenziato il relativo regime di pubblicità, prevedendo per gli atti formati dalla Commissione d'inchiesta la "pubblicazione" (art. 4, comma 1, lett. *m*), del Codice) su internet e per gli altri documenti la sola "comunicazione" degli stessi (art. 4, comma 1, lett. *l*), del Codice), nella forma della consultabilità a richiesta dei soggetti eventualmente interessati, assicurando in tal modo il pubblico interesse alla piena conoscibilità degli atti esterni acquisiti dalle Commissioni.

In tale cornice, è stato ritenuto che, per favorire una maggiore facilità di accesso agli atti esterni acquisiti dalle Commissioni parlamentari d'inchiesta, nel pieno rispetto dell'interesse alla loro massima conoscibilità, trattando le Commissioni d'inchiesta di questioni di "pubblico interesse", possono essere comunque predisposte

modalità di accesso *online* alle medesime informazioni, tramite accessi selettivi, ai soli soggetti che ne facciano richiesta appositamente identificati. Tale soluzione, che è stata rappresentata come un'opzione praticabile, deve ritenersi preferibile rispetto alla diffusione in quanto assicura un corretto bilanciamento tra le esigenze di semplificazione delle modalità di accesso a informazioni di "pubblico interesse" e il diritto alla protezione dei dati personali.

Al riguardo, per completezza è stato ricordato che il Cad, per consentire l'accesso ai servizi erogati in rete da parte delle pp.aa, prevede l'utilizzo della carta d'identità elettronica e della carta nazionale dei servizi, oppure di strumenti diversi purché idonei a consentire "l'individuazione del soggetto che richiede il servizio" (art. 64, commi 1 e 2, d.lgs. 7 marzo 2005, n. 82) (nota 19 giugno 2014).

4.5. *La documentazione anagrafica e la materia elettorale*

Per quanto riguarda la materia elettorale, il Garante ha adottato un nuovo provvedimento generale in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale (provv. 6 marzo 2014, n. 107, doc. web n. 3013267) che introduce notevoli profili di semplificazione per il trattamento dei dati personali.

Con il citato provvedimento viene introdotto uno specifico regime di esonero dall'obbligo di rendere l'informativa per partiti, movimenti politici, sostenitori e singoli candidati nel caso in cui si utilizzino dati personali estratti da particolari registri ed elenchi pubblici (ad es., liste elettorali ed assimilate). Le prescrizioni in materia di esonero, infatti, non hanno più, come in passato, vigenza provvisoria e circoscritta a determinate consultazioni (cfr. provv.ti 12 febbraio 2004, n. 45, doc. web n. 634369; 7 settembre 2005, n. 212, doc. web n. 1165613; 24 aprile 2013, n. 228, doc. web n. 2404305), ma sono applicabili ogni qual volta si svolgano consultazioni politiche, amministrative o referendarie, o iniziative per selezione di candidati (cd. primarie), nel rispetto di presupposti, condizioni e limiti, anche temporali, individuati con il predetto provvedimento. L'Autorità ha così inteso evitare che, nel breve arco temporale in cui si svolgono le consultazioni (politiche, amministrative o referendarie), un alto numero di interessati riceva un elevato numero di informative analoghe riguardanti il trattamento dei dati personali da parte di più soggetti impegnati in iniziative di comunicazione politica. Ciò in considerazione del fatto che i messaggi elettorali vengono generalmente inviati per posta all'indirizzo risultante dalle liste elettorali che, per una precisa scelta normativa, costituiscono la fonte privilegiata di dati personali lecitamente utilizzabili per i predetti fini (art. 51, d.P.R. 20 marzo 1967, n. 223, come modificato dall'art. 177, comma 5, del Codice).

Per ciò che concerne le modalità di utilizzo di dati personali estratti da fonti pubbliche – vale a dire le informazioni contenute in registri, elenchi, atti o documenti detenuti da un soggetto pubblico e al tempo stesso accessibili in base ad un'espressa disposizione di legge o di regolamento – viene ribadito che non è necessario richiedere il consenso degli interessati, ma occorre rispettare i limiti e le modalità eventualmente stabilite dall'ordinamento per accedere a tali fonti (ad es., se è richiesta l'identificazione di chi ne chiede copia o se l'accesso è consentito solo in determinati periodi o per determinate finalità) o per utilizzarle (ad es., obbligo di indicare la fonte dei dati o di rispettare le finalità che la legge stabilisce per determinati elenchi). Possono, pertanto, essere utilizzate le liste elettorali detenute presso i comuni (art. 51, d.P.R. 20 marzo 1967, n. 223, come modificato dall'art. 177, comma 5, del Codice), l'elenco degli elettori italiani che votano all'estero per

le elezioni del Parlamento europeo (art. 4, d.l. 24 giugno 1994, n. 408, convertito con l. 3 agosto 1994, n. 483), le liste aggiunte dei cittadini elettori di uno Stato membro dell'Unione europea residenti in Italia e che intendano ivi esercitare il diritto di voto alle elezioni del Parlamento europeo (artt. 1 e ss., d.lgs. 12 aprile 1996, n. 197), l'elenco provvisorio dei cittadini italiani residenti all'estero aventi diritto al voto (art. 5, comma 8, d.P.R. 2 aprile 2003, n. 104; per i Comitati degli italiani all'estero, art. 13, comma 2, l. 23 ottobre 2003, n. 286; art. 11, comma 2, d.P.R. n. 395/2003).

Anche alla luce delle segnalazioni pervenute nel corso degli anni, il provvedimento individua alcune fonti documentali detenute dai soggetti pubblici che non possono essere utilizzate per finalità di propaganda elettorale. Tra queste sono ricomprese: le Anagrafi comunali della popolazione residente (artt. 33 e 34, d.P.R. 30 maggio 1989, n. 223; art. 62, d.lgs. 7 marzo 2005, n. 82; d.P.C.M. 23 agosto 2013, n. 109), e ciò anche se il richiedente è un amministratore locale o il titolare di una carica elettiva che intenda utilizzarle ai predetti fini o per intrattenere pubbliche relazioni di carattere personale; gli archivi dello stato civile (art. 450 c.c.; d.P.R. 3 novembre 2000, n. 396); gli schedari dei cittadini residenti nella circoscrizione presso ogni ufficio consolare (art. 8, d.lgs. 3 febbraio 2011, n. 71); i dati raccolti dai soggetti pubblici nello svolgimento delle proprie attività istituzionali o, in generale, per la prestazione di servizi, gli elenchi di iscritti ad albi e collegi professionali (art. 61, comma 2, del Codice); gli indirizzi di posta elettronica tratti dall'indice nazionale degli indirizzi Pec delle imprese e dei professionisti (d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla l. 17 dicembre 2012, n. 221, che ha inserito l'art. 6-*bis* nel d.lgs. 7 marzo 2005, n. 82).

Viene, inoltre, ribadito il divieto di utilizzare le liste elettorali di sezione già utilizzate nei seggi, sulle quali sono annotati i dati relativi ai non votanti e che sono utilizzabili solo per controllare la regolarità delle operazioni elettorali (art. 62, d.P.R. 16 maggio 1960, n. 570), nonché i dati annotati nei seggi da scrutatori e rappresentanti di lista per lo svolgimento delle operazioni elettorali. Tali dati, se conosciuti, devono essere trattati con la massima riservatezza nel rispetto del principio costituzionale della libertà e della segretezza del voto, avuto anche riguardo alla circostanza che la partecipazione o meno ai *referendum* o ai ballottaggi può evidenziare di per sé anche un eventuale orientamento politico dell'elettore.

Non possono, parimenti, essere utilizzati i dati personali resi disponibili sui siti istituzionali dei soggetti pubblici sulla base di obblighi derivanti dalle disposizioni in materia di trasparenza delle informazioni concernenti l'organizzazione e l'attività delle pp.aa. (l. 18 giugno 2009, n. 69; d.lgs. 14 marzo 2013, n. 33), nonché da altre norme di settore. Si pensi, ad esempio, agli atti contenenti dati personali pubblicati sull'albo pretorio *online*, alla pubblicità degli esiti concorsuali, agli atti di attribuzione a persone fisiche di vantaggi economici comunque denominati, agli organigrammi degli uffici pubblici recanti anche recapiti telefonici e indirizzi di posta elettronica dei dipendenti, alle informazioni riferite agli addetti ad una funzione pubblica. La circostanza che tali dati siano resi pubblicamente conoscibili *online* per finalità di trasparenza non consente che gli stessi siano liberamente riutilizzabili da chiunque e per qualsiasi scopo, ivi compreso, quindi, il perseguimento di finalità di propaganda elettorale e connessa comunicazione politica.

Anche i dati acquisiti dai titolari di alcune cariche elettive per l'esercizio del mandato e la partecipazione alla vita politico-amministrativa dell'ente (art. 43, comma 2, d.lgs. 18 agosto 2000, n. 267), ovvero da chi riveste cariche pubbliche non elettive o, più in generale, incarichi pubblici, per lo svolgimento dei propri compiti istituzionali, non possono essere utilizzati per le finalità in esame. Come detto, la fina-

lizzazione esclusiva dei dati così ottenuti all'esercizio del mandato o allo svolgimento dei compiti istituzionali previsti dalla legge, costituisce, al tempo stesso, il presupposto che legittima l'accesso e che ne limita la portata.

Infine, il provvedimento ribadisce il divieto di utilizzo di particolari indirizzari o dati raccolti da strutture sanitarie, pubbliche e private, ovvero da singoli professionisti sanitari, nell'ambito delle attività di diagnosi e cura da essi svolti, al fine di veicolare messaggi di comunicazione politica volti a sostenere la candidatura di personale medico o comunque legato alla struttura sanitaria presso la quale l'interessato si è recato per fini di cura.

Anagrafe nazionale della popolazione residente

Per quanto riguarda la fase attuativa della nuova Anagrafe nazionale della popolazione residente (Anpr), istituita dall'art. 62 del Cad (introdotto dall'art. 2, comma 1, d.l. n. 179/2012, convertito dalla l. n. 221/2012), l'Autorità ha fornito il proprio parere sui decreti che definiscono i tempi e le modalità per l'istituzione della suddetta banca dati presso il Ministero dell'interno. Come è noto, l'Anpr subentra all'Indice nazionale delle anagrafi (Ina) e all'Anagrafe degli italiani residenti all'estero (Aire) nonché alle singole banche dati anagrafiche attualmente tenute dai comuni italiani, determinando in tal modo la centralizzazione presso il Ministero dell'interno di un numero cospicuo di informazioni personali.

L'Anpr è preordinata ad assicurare ai comuni la disponibilità dei dati anagrafici della popolazione residente per lo svolgimento delle funzioni di anagrafe e di stato civile, nonché i servizi informativi necessari per lo svolgimento delle altre funzioni istituzionali. Allo stesso modo, le altre pubbliche amministrazioni dovranno avvalersi dell'Anpr per la raccolta delle informazioni anagrafiche necessarie allo svolgimento dei propri compiti istituzionali. Le informazioni anagrafiche, una volta rese dagli interessati, si intendono acquisite anche dalle altre amministrazioni, senza necessità di ulteriori adempimenti in capo ai singoli, garantendo l'allineamento con le altre banche dati.

In tale percorso attuativo il Garante ha fornito le proprie indicazioni in ordine alle garanzie e alle misure di sicurezza da adottare per la raccolta e il trattamento dei dati, alle modalità e ai tempi di conservazione, all'esattezza ed all'integrità dei dati ed all'allineamento, nella prima fase, con i dati contenuti nelle banche dati dei comuni, alle modalità di accesso ai servizi resi dall'Anpr da parte dei comuni stessi e delle altre pp.aa, ai criteri per l'interoperabilità con le altre banche dati di interesse nazionale secondo le regole del sistema pubblico di connettività (parere 17 aprile 2014, n. 202, doc. web n. 3105794; d.P.C.M. 10 novembre 2014, n. 194, Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (Anpr) e di definizione del piano per il graduale subentro dell'Anpr alle anagrafi della popolazione residente, in *G.U.* 8 gennaio 2015, n. 5).

Il Garante è stato inoltre chiamato ad esprimere il parere sullo schema di decreto del Presidente della Repubblica in tema di "adeguamento del regolamento anagrafico della popolazione residente approvato con d.P.R. 30 maggio 1989, n. 223, alla disciplina istitutiva dell'Anagrafe nazionale della popolazione residente" (provv. 22 gennaio 2015, n. 31, doc. web n. 3738655).

Ancora con riferimento alla materia anagrafica, la Prefettura di Avellino, ha formulato un quesito in merito alla possibilità per il Dipartimento di prevenzione dell'Asl di Avellino di acquisire elenchi e vari dati anagrafici relativi ai cittadini residenti nei comuni della provincia, finalizzati al funzionamento del Registro provinciale dei tumori della popolazione. Al riguardo, l'Asl ha precisato che i dati dei comuni che rientrano nell'area di riferimento del Registro tumori risulterebbero necessari per verificare la correttezza delle anagrafi sanitarie e per rilevare il dettaglio degli indirizzi dell'intera popolazione di riferimento, indispensabile per gli

studi di epidemiologia ambientale. L'Ufficio, dopo aver ricordato che la disciplina sugli atti anagrafici consente di rilasciare, anche periodicamente, elenchi di iscritti nell'anagrafe della popolazione residente "alle amministrazioni pubbliche che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità", e che è anche previsto il rilascio di "dati 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), ha precisato che la prima delle finalità esplicitate – verifica della "correttezza delle anagrafi sanitarie" presenti nel Registro – può essere effettuata anche avvalendosi delle modalità di comunicazione telematica previste dall'art. 58, comma 2, del Cad. Per quanto riguarda, invece, la richiesta del dettaglio degli indirizzi dell'intera popolazione di riferimento, indispensabile per gli studi di epidemiologia ambientale, è stato evidenziato che tale esigenza deve essere valutata alla luce delle specifiche disposizioni che prevedono "la raccolta, l'elaborazione e la registrazione di dati statistici completi [...] dei casi di tumore anche infantili che si verificano nella popolazione della Regione Campania", ovvero "dei dati individuali, sanitari ed amministrativi, sugli ammalati di tumore", e non dell'intera popolazione del territorio di competenza (cfr. art. 1, comma 2 lett. *a*) e art. 3, comma 1, l.r. 10 luglio 2012, n. 19, concernente l'istituzione del Registro tumori della popolazione della Regione Campania). Infine, dopo aver richiamato il quadro normativo di riferimento per i trattamenti per scopi statistici e scientifici (artt. 104 e ss. del Codice, All. A.4, codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, doc. web n. 1556635), è stato puntualizzato che l'acquisizione di dati ed altre informazioni anagrafiche relativi all'intera popolazione è consentita per lo svolgimento di specifici scopi scientifici – tra i quali rientrano anche gli studi epidemiologici – purché "chiaramente determinati" e specificamente indicati in relazione alla singola richiesta (art. 105 del Codice). Tali scopi devono, inoltre, essere resi noti agli interessati nei modi previsti dall'art. 13 del Codice ed il trattamento successivo alla raccolta non deve permettere di identificare gli interessati, anche indirettamente, salvo che l'abbinamento al materiale di ricerca dei dati identificativi dell'interessato sia temporaneo ed essenziale per il risultato della ricerca, e sia motivato, altresì, per iscritto (art. 105, commi 2 e 4, del Codice) (nota 15 settembre 2014).

4.6. *L'istruzione scolastica ed universitaria*

Risultano sempre numerosi i chiarimenti richiesti in relazione al trattamento di dati personali effettuato nell'ambito dell'istruzione scolastica ed universitaria.

Con riferimento ai dati pubblicati tramite gli albi scolastici, è stato segnalato al Garante che un istituto statale comprensivo ha affisso agli albi delle scuole ed alle bacheche esterne dei plessi il testo di una comunicazione elettronica, nell'ambito della quale risultava visibile l'indirizzo di posta elettronica privato di uno dei destinatari, docente presso l'istituto medesimo.

Al riguardo, è stato ribadito che i soggetti pubblici possono diffondere dati personali, diversi da quelli sensibili e giudiziari, unicamente quando tale specifica operazione di trattamento risulta ammessa da una norma di legge o di regolamento (art. 19, comma 3, del Codice). Ciò posto, l'Autorità, considerato che l'indirizzo di posta elettronica costituisce dato personale, ai sensi dell'art. 4, comma 1, lett. *b*), del Codice, e che la citata operazione di trattamento integra una diffusione di dati di dati personali, ai sensi dell'art. 4 comma 1, lett. *m*), del Codice, dopo aver constatato l'assenza di una base normativa che legittimasse la citata operazione di trattamento, ha

rilevato l'illiceità della predetta diffusione ed ha vietato all'istituto l'ulteriore diffusione, con qualunque mezzo, ivi compresa l'affissione all'albo ed alle bacheche delle scuole, del dato relativo all'indirizzo di posta elettronica personale del segnalante (provv. 23 gennaio 2014, n. 28, doc. web n. 2929890).

Un'altra segnalazione ha riguardato un istituto scolastico statale che, nel documento di programmazione di una classe, al capitolo programmazione alunni dislessici, aveva riportato i nominativi degli alunni affetti da disturbi specifici dell'apprendimento (dsa).

Al riguardo, l'Ufficio ha evidenziato che le istituzioni scolastiche pubbliche possono trattare dati sensibili, tra i quali rilevano quelli idonei rivelare lo stato di salute, solo se autorizzati da espressa disposizione di legge nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Nei casi in cui la legge, pur specificando la finalità di rilevante interesse pubblico, non evidenzi, altresì, i tipi di dati sensibili e giudiziari e di operazioni eseguibili, il trattamento è consentito, nel rispetto dei principi di cui all'art. 22 del Codice, ed, in particolare, del principio di indispensabilità, solo per lo svolgimento di specifiche finalità, in riferimento ai tipi di dati e di operazioni identificati e resi pubblici dal titolare in un atto di natura regolamentare adottato in conformità al parere espresso dal Garante (artt. 20 e 22 del Codice; l. 8 ottobre 2010, n. 170; d.m. 12 luglio 2011, n. 5669).

Su tali basi, l'Ufficio ha rilevato la non conformità della predetta condotta alla disciplina in materia di protezione dei dati personali, nella misura in cui non è risultato effettivamente indispensabile alle finalità perseguite l'indicazione dei nominativi degli studenti affetti da dsa nel citato documento. Anche in questo caso, tuttavia, l'Ufficio non ha promosso l'adozione di un provvedimento da parte del Collegio, tenuto conto del fatto che la condotta aveva esaurito i suoi effetti e delle rassicurazioni fornite dal titolare del trattamento circa l'immediato oscuramento dei predetti dati personali dal documento di programmazione della classe (nota 8 gennaio 2014).

È stato inoltre segnalato che una scuola superiore di secondo grado ha diffuso sul proprio sito internet istituzionale gli elenchi degli alunni, distinti per classe, per supposte finalità di trasparenza (art. 19, comma 3, del Codice).

A seguito della richiesta di chiarimenti avanzata dall'Ufficio, l'istituto scolastico ha provveduto all'immediata cancellazione dei predetti elenchi. Al riguardo, è stato, infatti evidenziato che tali dati non rientrano tra quelli oggetto di pubblicazione obbligatoria per finalità di trasparenza, ai sensi del d.lgs. n. 33/2013, ed è stato ribadito che la diffusione di dati personali da parte di soggetti pubblici è ammessa unicamente quando è prevista da una norma di legge o di regolamento, nel rispetto del principio di pertinenza e non eccedenza (art. 19, comma 3, e art. 11, comma 1, lett. *d*), del Codice) e che, quindi, le amministrazioni, prima di diffondere sui propri siti istituzionali atti e documenti contenenti dati personali, devono verificare che esista una norma di legge o di regolamento che ne preveda l'obbligo di pubblicazione (punto 2, provv. 15 maggio 2014, n. 243, doc. web n. 3134436; nota 8 gennaio 2015).

Giudizi relativi ai partecipanti alla procedura di abilitazione scientifica nazionale

Nell'ambito dell'attività dell'Ufficio è emerso che il Ministero dell'istruzione, dell'università e della ricerca ha diffuso sul proprio sito internet istituzionale gli atti e i giudizi individuali, anche negativi, relativi ai singoli partecipanti alla procedura di abilitazione scientifica nazionale per l'accesso al ruolo dei professori universitari, a norma dell'art. 16, l. 30 dicembre 2010, n. 240, consentendone, altresì, la reperibilità anche attraverso i più comuni motori di ricerca generalisti (quali Google).

Come detto, il Codice dispone che i soggetti pubblici, nell'ambito delle proprie competenze istituzionali, possono diffondere dati personali solo qualora tale operazione di trattamento sia ammessa da una norma di legge o di regolamento. La dif-

fusione, nel rispetto dei principi di necessità e proporzionalità, può durare solo per il tempo necessario allo scopo per il quale è stata effettuata (artt. 3, 11, 18 e 19, comma 3, del Codice).

Con riferimento alla diffusione dei giudizi, anche negativi, sui singoli candidati, è emerso che tale specifica operazione di trattamento è espressamente prevista, per un periodo di 120 giorni, dall'art. 16, l. n. 240/2010 e dall'art. 8, comma 9, d.P.R. n. 222/2011 (Regolamento concernente il conferimento dell'abilitazione scientifica nazionale per l'accesso al ruolo dei professori universitari, a norma dell'art. 16, l. 30 dicembre 2010, n. 240). La circostanza che tale diffusione possa, legittimamente, concernere anche i giudizi negativi dei singoli candidati è stata altresì motivata alla luce dei pareri forniti dal Consiglio di Stato in sede consultiva sul predetto regolamento, in base ai quali tali procedure, consentendo l'accesso a ruoli di estremo valore culturale, devono essere improntate alla massima trasparenza per consentire il controllo diffuso dell'intera comunità scientifica.

Con riferimento, invece, alla reperibilità anche attraverso i più comuni motori di ricerca generalisti, dei giudizi individuali dei candidati, accertato che tale possibilità risulta sproporzionata rispetto alle finalità del trattamento, a seguito dell'intervento dell'Autorità ed al fine di garantire un elevato *standard* di tutela del diritto alla protezione dei dati personali nell'ambito del trattamento in esame, il Ministero ha assicurato la rimozione dell'indicizzazione della pagine riportanti i risultati dell'abilitazione scientifica nazionale e l'implementazione di idonee misure atte ad impedire nuove indicizzazioni simili (nota 1° luglio 2014).

Archivio "Andrea Devoto"

Un interessante caso ha riguardato l'Università degli Studi di Firenze che ha in concessione il noto Archivio "Andrea Devoto", di proprietà della Regione Toscana, contenente le interviste che negli anni 80 il neuropsichiatra e psicologo Andrea Devoto rivolse, nell'ambito di uno studio, ad alcuni deportati sopravvissuti ai campi di sterminio nazisti. Da tali interviste emergono ovviamente dati sensibili, idonei a rivelare lo stato di salute degli intervistati dopo la deportazione.

Ciò posto, l'Ateneo ha formulato un quesito circa la possibilità di rendere consultabili i materiali contenuti nell'Archivio Devoto ed eventualmente consentire la pubblicazione delle interviste, procedendo alla cancellazione dei nominativi degli interessati.

Al riguardo, l'Ufficio ha evidenziato che il Codice in materia di protezione dei dati personali rinvia al codice dei beni culturali e del paesaggio (d.lgs. 22 gennaio 2004, n. 42) per l'individuazione della disciplina relativa alla consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati (art. 103 del Codice; art. 122, comma 1, lett. *b*) e 126, comma 3, del codice dei beni culturali e del paesaggio, cit.). Inoltre, in base al codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, All. A.2 al Codice (adottato ai sensi dell'art. 102 del Codice) – la cui osservanza costituisce condizione essenziale per la liceità dei trattamenti di dati personali per la predetta finalità – l'accesso agli archivi pubblici è libero, con eccezione dei documenti di carattere riservato relativi alla politica interna ed estera dello Stato che divengono consultabili cinquanta anni dopo la loro data, e quelli contenenti i dati personali, sensibili e giudiziari, che divengono liberamente consultabili quaranta anni dopo la loro data. Il termine è di settanta anni se i dati sono idonei a rivelare lo stato di salute o la vita sessuale oppure rapporti riservati di tipo familiare (art. 10, commi 1 e 2, codice di deontologia; art. 122, comma 1, lett. *b*), del codice dei beni culturali e del paesaggio, cit.).

Con riferimento, invece, alla possibilità che le interviste dei pazienti vengano diffuse adottando accorgimenti idonei a rendere non identificabili gli intervistati, ad es. cancellando i nominativi degli stessi, è stato evidenziato che la semplice cancel-

lazione degli identificativi diretti non è una tecnica idonea a garantire (con certezza) l'anonimizzazione dei dati personali. Infatti, fintantoché persistano elementi sufficienti per consentire l'identificazione della persona interessata, le informazioni trattate devono considerarsi dati personali, ancorché indirettamente identificativi, e come tali soggetti alla specifica disciplina di settore sopra richiamata (artt. 4, comma 1, lett. *b*) e *n*), del Codice).

È stato, altresì, evidenziato che il Ministro dell'interno, previo parere del direttore dell'Archivio di Stato o del sovrintendente archivistico competenti e udita la Commissione per le questioni inerenti alla consultabilità degli atti di archivio riservati istituita presso il Ministero dell'interno, può rilasciare l'autorizzazione alla consultazione dei documenti riservati prima dei termini sopra indicati agli utenti che presentino uno specifico progetto di ricerca. Tale autorizzazione, che è personale e non delegabile a soggetti terzi, può contenere specifiche cautele volte a tutelare i diritti, la libertà e la dignità delle persone interessate (art. 10, del menzionato codice di deontologia; artt. 123 e 126, comma 3, del codice dei beni culturali e del paesaggio). L'Ufficio ha ricordato, infine, che gli archivisti possono trattare i documenti conservati negli archivi contenenti dati personali, in conformità alle regole generali di condotta individuate nel citato codice di deontologia volte, in particolare, a favorire il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone alle quali si riferiscono i dati trattati (nota 17 settembre 2014).

4.7. *L'attività fiscale e tributaria*

È stato definito un reclamo concernente un trattamento di dati personali effettuato dall'Agenzia delle entrate di Latina nell'ambito di un accertamento tributario. Ritenuto il prezzo dichiarato in atti non congruo in relazione alle quotazioni della banca dati dell'Osservatorio del mercato immobiliare (Omi), l'Agenzia notificava ad un soggetto terzo un avviso di rettifica e liquidazione, che riportava in motivazione informazioni personali relative alla reclamante (ed in particolare che la stessa, dante causa dell'immobile in questione, non si era presentata a fornire dati e notizie relativamente ai rapporti finanziari, al fine di giustificare l'ammontare del saldo passivo di tali movimentazioni). L'istruttoria ha evidenziato che le indagini bancarie effettuate dalla menzionata Agenzia erano necessarie per acquisire elementi probatori utili a ricostruire il corrispettivo dichiarato nell'atto di cessione del fabbricato, che rilevava uno scostamento superiore al 50% alle rilevazioni della banca dati Omi e che la motivazione dell'avviso di liquidazione, di conseguenza, doveva evidenziare le informazioni reperite a seguito delle predette indagini finanziarie al fine di sostenere la pretesa tributaria. Tanto premesso, l'Ufficio ha ritenuto leciti e conformi ai principi di pertinenza e non eccedenza, i trattamenti di dati personali effettuati dall'Agenzia delle entrate. Con riferimento alla tipologia dei dati personali riportati nella motivazione dell'atto, la normativa di settore prevede, infatti, che l'avviso di rettifica e di liquidazione della maggiore imposta "deve indicare i presupposti di fatto e le ragioni giuridiche che lo hanno determinato" e che "l'accertamento è nullo se non sono osservate le disposizioni di cui al presente comma" (art. 52, comma 2, d.P.R. n. 131/1986). Infine, data la natura solidale dell'obbligazione tributaria in questione (art. 57, d.P.R. n. 131/1986, per l'imposta di registro; art. 11, d.lgs. n. 347/1990, per l'imposta ipotecaria e catastale), l'atto di accertamento dell'amministrazione finanziaria poteva essere notificato a ciascuno dei coobbligati, tutti legittimati a conoscerne il contenuto; di conseguenza, è stata ritenuta lecita la comunicazione dei dati della reclamante ai predetti (nota 17 ottobre 2014).

Il Garante, su richiesta del Consiglio di Stato, ha fornito al Ministero dell'economia e delle finanze un parere sul nuovo schema di Contratto di servizi quadro 2012-2017, regolante il rapporto per la gestione *in house* del sistema informativo della fiscalità tra l'Amministrazione finanziaria nel suo complesso e la Sogei S.p.A., quale suo ente strumentale preposto al settore dell'*Information and Communication Technology*.

Al riguardo, il Garante, vista l'estrema delicatezza dei dati personali trattati nell'ambito del sistema informativo della fiscalità, nonché il rilevante valore economico dell'affidamento, ha fornito al Ministero alcune indicazioni relative alle previsioni contrattuali in modo da assicurare all'amministrazione un maggior livello di prestazione relativamente ai servizi aventi un diretto impatto sulla sicurezza e sulla protezione dei dati personali, quali la protezione perimetrale, il rilevamento di intrusioni e il "*disaster recovery*". Sono state inoltre fornite indicazioni riguardo ai trattamenti di dati personali che possono avere luogo a seguito dell'adozione di strumenti di filtraggio della c.d. navigazione web (provv. 13 febbraio 2014, n. 68 doc. web n. 3001879).

4.8. *La videosorveglianza in ambito pubblico*

Come già avvenuto negli ultimi anni l'Autorità è stata più volte chiamata a esprimersi in ordine al trattamento di dati personali effettuato tramite sistemi di videosorveglianza in ambito pubblico. In particolare, nel dare riscontro ad un comune, l'Ufficio ha fornito i necessari chiarimenti sulla durata della conservazione delle immagini registrate, facendo presente che per i comuni, e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, il termine massimo di durata della conservazione dei dati è limitato ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte, fatte salve speciali esigenze di ulteriore conservazione (cfr. punto 3.4, provv. 8 aprile 2010, doc. web n. 1712680; art. 6, comma 8, d.l. 23 febbraio 2009, n. 11 convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 23 aprile 2009, n. 38) (nota 25 marzo 2014).

Ove si intenda, invece, conservare le immagini registrate per un periodo superiore alla settimana, l'Ufficio ha ricordato ad un istituto scolastico che una richiesta in tal senso deve essere sottoposta ad una verifica preliminare dell'Autorità, ai sensi dell'art. 17 del Codice, e che la congruità di un termine più ampio di conservazione va adeguatamente motivata facendo riferimento ad una specifica esigenza di sicurezza, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità (cfr. punto 3.4. del citato provvedimento generale) (nota 19 dicembre 2014).

Sempre con riferimento alla durata della conservazione delle immagini registrate, un centro di ricerca privato aveva richiesto, attraverso la verifica preliminare del Garante (art. 17 del Codice), di poter allungare i tempi di conservazione delle immagini registrate presso le aree interne del centro per un periodo di trenta anni, in corrispondenza alla durata di un progetto di ricerca effettuato dallo stesso. Considerata la peculiarità dell'istanza, sono stati chiesti chiarimenti, anche in occasione di un incontro tenutosi presso la sede dell'Ufficio, volti a conoscere se, nell'ambito dell'attività di monitoraggio del processo lavorativo relativo al progetto di ricerca, le telecamere rilevassero o meno immagini dei lavoratori in modo da renderli identificabili. Alla luce delle indicazioni fornite durante il citato incontro, il centro di ricerca ha sospeso la richiesta di verifica preliminare riservandosi di presentare una nuova richiesta, formulata all'esito delle necessarie valutazioni (note 5 giugno e 24 dicembre 2014).

Diversi sono stati poi gli aspetti presi in considerazione nel fornire indicazioni ad alcuni comuni che avevano attivato sistemi di videosorveglianza nell'ambito delle attività di controllo amministrative.

In un caso (cfr. nota 25 marzo 2014) è stato rilevato che l'utilizzo di sistemi di videosorveglianza risulta lecito per accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose nonché per monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente, solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi (art. 13, l. 24 novembre 1981, n. 689).

È stata altresì esaminata una segnalazione con la quale si lamentava la comunicazione da parte di un comune ad un'emittente televisiva di alcuni dati personali contenuti nelle immagini riprese da sistemi di videosorveglianza comunale relative a cittadini che conferivano in modo non conforme i rifiuti. Il comune, interpellato dall'Ufficio, ha chiarito che i cittadini ripresi non erano riconoscibili, in quanto non ne venivano mostrati chiaramente i volti; né poteva desumersi la residenza dei presunti trasgressori soltanto dalle immagini relative alla via della città ove le telecamere erano installate. Pertanto, l'Ufficio non ha ravvisato gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali (nota 19 gennaio 2015).

In un altro caso, sempre nell'ambito dell'attività di controllo comunale, è stata avviata un'istruttoria nei confronti di un comune di rilevanti dimensioni, il cui corpo di polizia locale aveva attivato un *account* su *Twitter* al fine di ricevere segnalazioni da parte dei cittadini in ordine a problematiche legate alla cd. "sosta selvaggia" e a situazioni di degrado o di insicurezza urbana. Dall'istruttoria preliminare era risultato che, talvolta, i segnalanti allegavano ai loro messaggi fotografie o video che riprendevano veicoli, dei quali fosse visibile la targa di immatricolazione. Pertanto sono stati chiesti al comune elementi di valutazione in ordine alle cautele da adottare, al fine di evitare la diffusione di dati personali non pertinenti ed eccedenti rispetto alla finalità perseguita (nota 11 marzo 2014).

Alla luce di quanto richiesto, il comune ha dichiarato di voler spostare su una piattaforma web, già progettata e in via di acquisizione, la gestione delle segnalazioni che consentirà agli utenti di relazionarsi in maniera riservata con la centrale operativa del comando generale; l'Ufficio ha chiesto di essere informato in merito alla soluzione prescelta, manifestando disponibilità a collaborare (nota 16 giugno 2014).

Impianti elettronici di rilevamento delle violazioni del codice della strada

In relazione poi alla funzione istituzionale comunale dell'accertamento delle violazioni al codice della strada, a seguito di una segnalazione, l'Ufficio ha avuto modo di fornire indicazioni ad un comune sul corretto utilizzo degli impianti elettronici di rilevamento delle infrazioni, sulle modalità con le quali consentire la consultazione sul web delle infrazioni e sulla durata della conservazioni delle immagini a tal fine rilevate. In particolare, è stato evidenziato che l'utilizzo di impianti elettronici di rilevamento automatizzato delle infrazioni è lecito se sono raccolte solo immagini pertinenti e non eccedenti (o inutilmente dettagliate) per il perseguimento della finalità di accertamento del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese.

In particolare, è stato evidenziato che le risultanze fotografiche o le riprese video possono individuare unicamente gli elementi previsti dalla normativa di settore per la predisposizione del verbale di accertamento delle violazioni (ad es., ai sensi dell'art. 383, d.P.R. n. 495/1992, il tipo di veicolo, il giorno, l'ora e il luogo nei quali la violazione è avvenuta) e che, pertanto, deve essere effettuata una ripresa del veicolo che non comprenda o, in via subordinata, mascheri, per quanto possibile, la porzione delle risultanze video/fotografiche riguardanti soggetti non coinvolti nel-

l'accertamento amministrativo (cfr. punto 5.3.1. del provvedimento generale). Va evitato, in ogni caso, che tale documentazione video-fotografica riguardante i soggetti non coinvolti sia messa a disposizione del destinatario del verbale di contestazione della violazione.

Al comune è stato quindi richiesto di valutare la pertinenza e non eccedenza dei dati personali contenuti nelle risultanze fotografiche visualizzabili nella pagina web del comune, anche con riferimento ad infrazioni molto risalenti nel tempo, a carico di un determinato numero di targa, nonostante l'avvenuto pagamento della sanzione e l'assenza di contenzioso al riguardo, tenuto anche della circolare del Ministero dell'interno del 14 agosto 2009, n. 300/A/10307/09/144/5/20/3 (par. n. 6 dell'All. n. 1), che prevede che "le immagini siano conservate solo per il periodo di tempo strettamente necessario all'applicazione delle sanzioni e alla definizione dell'eventuale contenzioso" (nota 18 luglio 2014). A seguito dell'intervento dell'Ufficio, il comune ha comunicato di aver previsto idonee misure volte ad oscurare le targhe dei veicoli non coinvolti nell'accertamento ma eventualmente oggetto di ripresa e a rimuovere dalla pagina web del comune le immagini relative all'accertamento della violazione, decorso il termine di eventuale presentazione del ricorso decorrente dalla notificazione dell'infrazione al trasgressore (nota 12 dicembre 2014).

Videosorveglianza cd. intelligente

L'Ufficio si è occupato di valutare le richieste di verifica preliminare pervenute in relazione a trattamenti di dati personali effettuati tramite sistemi di videosorveglianza cd. intelligenti.

In particolare, si segnala la richiesta di verifica preliminare formulata dalla Banca d'Italia in relazione ad un sistema destinato ad essere installato presso le sedi dell'amministrazione e delle filiali per garantire la sicurezza degli edifici e dei beni dell'istituto, considerati i rischi specifici connessi allo stoccaggio e alla gestione di elevate quantità di valori.

In primo luogo, è stato verificato che, alla luce di taluni specifici compiti assegnati alla Banca d'Italia (emissione delle banconote in euro e servizio di Tesoreria provinciale e centrale dello Stato), la stessa persegue legittime finalità di sicurezza degli edifici e dei beni, anche attraverso l'istallazione di sistemi di videosorveglianza.

Differenti erano le funzionalità del sistema prospettate dalla Banca d'Italia; al riguardo, è stato precisato che tra le stesse, soltanto quelle di "controllo ambientale" connesse alla generazione di eventi d'allarme a fronte del superamento di una "barriera allarme virtuale", dell'accesso ad una "zona di allarme virtuale", nonché del "riconoscimento presenza persone" comportavano un trattamento di dati personali correttamente sottoposto alla verifica preliminare dell'Autorità in quanto risultavano idonee a rilevare automaticamente, segnalare e registrare comportamenti o eventi anomali, quali possono considerarsi gli accessi nelle zone interdette anche in relazione a determinate fasce orarie (cfr. punto 3.2.1 del predetto provvedimento generale).

L'Autorità ha, invece, ritenuto che altre funzionalità ("lettura targhe e identificazione mezzi", "*motion detection* digitale", "automazione accesso su chiamata citofonica", "conteggio", "riconoscimento oggetto abbandonato" e "mancanza oggetto") non rientrassero tra le ipotesi previste dal provvedimento generale in cui è necessario sottoporre i sistemi di videosorveglianza alla verifica preliminare. Ciò in quanto, per le funzioni di "lettura targhe e identificazione mezzi", "*motion detection* digitale", "automazione accesso su chiamata citofonica" e "conteggio" non è prevista la generazione di allarmi; in relazione alle funzioni di "riconoscimento oggetto abbandonato" e "mancanza oggetto", che prevedono, rispettivamente, l'attivazione di un allarme se un oggetto viene abbandonato all'interno dell'inquadratura di una o più telecamere per un determinato periodo di tempo e se un oggetto esistente viene rimosso dall'inquadratura, non riguardando persone, non comportano un trattamento di dati personali.

Analizzando, allora, nel merito il trattamento dei dati personali effettuato mediante le funzioni correttamente sottoposte alla verifica preliminare dell'Autorità, il Garante lo ha ritenuto proporzionato e quindi ammissibile, non riscontrando, in concreto, un pregiudizio rilevante per gli interessati, tale da determinare effetti particolarmente invasivi sulla loro sfera di autodeterminazione e, conseguentemente, sui loro comportamenti. Le caratteristiche specifiche dei sistemi in esame, infatti, nel rilevare il superamento di una barriera virtuale, delimitata da una linea predefinita, e l'accesso ad una zona interdetta segnalata da idonei cartelli informativi e dispositivi di delimitazione delle zone protette nonché il procedere nel senso contrario in un percorso predefinito, producevano il solo effetto di richiamare l'attenzione degli addetti al posto di controllo, al fine di favorirne un eventuale tempestivo intervento, volto a verificare la fondatezza della segnalazione d'allarme.

Infatti, dalla documentazione trasmessa era risultato che tali sistemi di videosorveglianza non attivavano ulteriori funzionalità, anche eventualmente legate al comportamento dell'interessato ripreso, quali l'analisi audio, la geolocalizzazione o il riconoscimento tramite incrocio con ulteriori specifici dati personali, anche biometrici, o il confronto con una campionatura precostituita.

L'Autorità ha, tuttavia, richiamato l'attenzione della Banca d'Italia sulle prescrizioni relative alle misure minime di sicurezza, con particolare riferimento all'obbligo di adottare specifici accorgimenti tecnici ed organizzativi che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (cfr. punto 3.3.1 del provvedimento generale; artt. 31-36 del Codice e All. B. al Codice), nonché sulle indicazioni in materia di informativa gli interessati (cfr. punto 3.1. del citato provvedimento generale; art. 13 del Codice). Inoltre, sebbene, secondo quanto dichiarato, i sistemi di videosorveglianza in esame non fossero in alcun modo finalizzati ad un controllo dell'attività dei lavoratori, qualora tale attività di videosorveglianza potesse in concreto aver luogo (pur non essendo a tal fine preordinata) il Garante ha evidenziato l'esigenza del rispetto delle garanzie previste per i lavoratori (punto 4.1; art. 114 del Codice; art. 4, l. n. 300/1970) (provv. 22 maggio 2014, n. 259, doc. web n. 3230814).

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

Nel caso di una segnalazione concernente una videoregistrazione di una seduta del consiglio comunale da parte di un consigliere senza aver previamente fornito ai presenti le informazioni di cui all'art. 13 del Codice, è stato evidenziato 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 pubblici, salvi i casi previsti dal regolamento. Pertanto, spetta 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). Nell'ipotesi in cui sia prevista la possibilità di effettuare le registrazioni video delle sedute del consiglio comunale, si evidenzia la necessità che agli interessati sia fornita, da parte del comune, l'informativa prevista dall'art. 13 del Codice (nota 3 aprile 2014).

L'Ufficio è intervenuto in più occasioni a seguito di segnalazioni concernenti le modalità di apertura e protocollazione della corrispondenza indirizzata nominativamente a consiglieri comunali presso il comune di appartenenza. In un caso si trattava di corrispondenza proveniente dalla Soprintendenza dei beni e delle attività culturali e del turismo, trasmessa in riscontro ad un esposto presentato dallo stesso consigliere comunale. In un altro caso, la consegna di una nota del Ministero del-

l'interno aperta, protocollata e con la busta spillata, perveniva in risposta ad un quesito del consigliere relativo alla eventuale ineleggibilità di un dipendente dell'unione di comuni alla carica di sindaco di uno degli enti facenti parte dell'unione. In entrambe le occasioni si è ritenuta la correttezza delle procedure operative osservate dal personale addetto all'apertura, protocollazione e distribuzione della corrispondenza in conformità alle specifiche regole stabilite nei manuali di gestione del protocollo informatico, della gestione dei flussi documentali e dell'archivio, approvati dai predetti comuni. Nei predetti casi, inoltre, la corrispondenza era inerente allo svolgimento delle funzioni istituzionali dei consiglieri comunali e non aveva carattere personale, attenendo alla sfera pubblica e alla carica rivestita, e non alla vita privata degli stessi (note 11 giugno e 1° settembre 2014).

Raccolta differenziata dei rifiuti solidi urbani

È tornata di grande attualità la tematica relativa al trattamento dei dati personali effettuato nell'ambito delle modalità di controllo delle procedure di raccolta differenziata dei rifiuti solidi urbani; ciò ha richiesto l'intervento dell'Ufficio, il quale, su impulso di cittadini o associazioni di consumatori e di amministratori di condominio, ha ricordato le prescrizioni contenute nel provvedimento generale del 14 luglio 2005 (doc. web n. 1149822).

In particolare, in relazione all'utilizzo di sacchetti trasparenti per la raccolta differenziata cd. porta a porta, è stata richiamata l'attenzione sulla prescrizione che considera, in termini generali, non proporzionato l'obbligo di utilizzare un sacchetto trasparente nella raccolta porta a porta, in quanto chiunque si trovi a transitare sul pianerottolo o nell'area antistante l'abitazione può visionare agevolmente il contenuto del sacchetto (note 23 maggio e 4 luglio 2014). In un caso, un comune ha fornito riscontro a quanto richiesto dall'Ufficio, comunicando di aver provveduto a sostituire le forniture dei sacchetti trasparenti utilizzati per la raccolta differenziata.

Sullo stesso argomento, l'Ufficio ha avuto occasione di chiarire in quale caso debba ritenersi applicabile il citato provvedimento del Garante, tenuto conto della diversità delle tipologie di sacchetti e della loro qualificazione (opachi, trasparenti, semi-trasparenti, translucidi): è stato, infatti, precisato che il provvedimento generale del 2005, volto a bilanciare il rispetto della disciplina sulla raccolta differenziata e il diritto degli interessati a non subire violazioni ingiustificate della propria sfera di riservatezza, trova applicazione qualora i sacchetti utilizzati nella raccolta porta a porta siano idonei a mostrare il contenuto degli stessi e, in particolare, effetti personali, che sono talvolta relativi ad informazioni concernenti la sfera della salute o di natura politica, religiosa o sindacale degli interessati (nota 2 gennaio 2015).

In un'altra circostanza, invece, non è stata ravvisata una violazione della disciplina in materia di protezione dei dati personali nel caso di un comune che aveva previsto un servizio telefonico per richiedere la raccolta a domicilio di pannolini e pannoloni per incontinenti e portatori di handicap, in quanto tale previsione costituiva una modalità di prelievo dei citati rifiuti attivabile solo a richiesta degli interessati; dalla documentazione in atti, infatti, non risultava che tale servizio gratuito fosse obbligatorio o esclusivo, essendo contemplata la possibilità che i suddetti materiali potessero essere versati nei sacchetti o nei bidoni riservati ai rifiuti appartenenti alla tipologia "secco residuo non riciclabile" (nota 23 maggio 2014).

Ad una associazione che segnalava la presunta violazione della normativa in materia di protezione dei dati personali da parte di un comune che imponeva per la raccolta dei rifiuti dei sacchetti contenenti un *microchip* identificativo, è stato ricordato che deve ritenersi lecito fornire agli utenti appositi sacchetti, da utilizzare obbligatoriamente per una determinata tipologia di materiale, dotati di *microchip* o, eventualmente, di dispositivi *Radio frequency identification* (Rfid) collegati ai dati identificativi del soggetto cui il contenitore si riferisce. Tale procedura consente di delimitare l'i-

dentificabilità del conferente ai soli casi in cui sia stata accertata la mancata osservanza delle prescrizioni in ordine alla differenziazione. Infatti, al momento dell'apertura del sacchetto, i soggetti preposti alla verifica dell'omogeneità dei materiali inseriti, che comunque sono tenuti al rispetto della riservatezza, vengono a conoscenza del contenuto, ma non anche, in prima battuta, degli elementi identificativi del soggetto conferente. Invece, i soggetti preposti all'applicazione della sanzione, mediante la decodifica del codice a barre o del *microchip*, acquisiscono il nominativo del soggetto cui il sacchetto si riferisce, solo in relazione alla non conformità del contenuto del sacchetto (cfr. punto 4.*c*) del citato provvedimento generale) (nota 25 giugno 2014).

L'Ufficio ha altresì risposto ad un quesito formulato da una università in merito alla possibilità di comunicare ad una società partecipata da più comuni che svolge servizi pubblici locali in materia ambientale dati personali di taluni studenti che si ritenevano essere responsabili dell'abbandono di rifiuti sul suolo pubblico a seguito dei festeggiamenti di laurea, in quanto i nomi degli stessi comparivano nei cartelloni esposti durante i suddetti festeggiamenti. In tale circostanza l'Ufficio ha rilevato un principio, già evidenziato nel provvedimento generale del 2005, secondo il quale agli organi addetti al controllo è riconosciuta la possibilità di procedere a ispezioni di cose e luoghi diversi dalla privata dimora per accertare le violazioni di rispettiva competenza (art. 13, l. 24 novembre 1981, n. 689), avendo cura di esercitare tale riconosciuta facoltà selettivamente, nei soli casi in cui il soggetto che abbia conferito i rifiuti con modalità difformi da quelle consentite non sia in altro modo identificabile. Risulterebbe quindi invasiva la pratica di ispezioni generalizzate da parte del personale incaricato (agenti di polizia municipale; dipendenti di aziende municipalizzate) del contenuto dei sacchetti al fine di rinvenire elementi in grado di identificare, presuntivamente, il conferente. L'attività di ispezione non costituisce strumento di per sé risolutivo per accertare l'identità del soggetto produttore e il trasgressore non dovrebbe essere individuato sempre ed esclusivamente attraverso una ricerca nei rifiuti di elementi a lui riconducibili; una eventuale sanzione amministrativa irrogata ad un soggetto così individuato potrebbe quindi risultare erroneamente comminata (cfr. punto 4.*d*) del provvedimento generale). Pertanto, la società che svolge servizi pubblici locali in materia ambientale può svolgere l'attività di controllo prevista dalla soprarichiamata l. n. 689/1981 nel rispetto dei limiti indicati nel citato provvedimento generale (nota 8 gennaio 2014).

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

Il Garante è stato consultato dall'Autorità per le garanzie nelle comunicazioni in merito alla possibilità di avvalersi delle modalità previste dall'art. 58, comma 2, del Cad per la fruibilità informatica di dati presenti nell'Anagrafe tributaria, al fine di verificare la correttezza delle dichiarazioni rese ai sensi degli artt. 46 e 47, d.P.R. 28 dicembre 2000, n. 445, nell'ambito della funzioni di controllo connesse alla tenuta del Registro degli operatori di comunicazione (istituito con l. 5 agosto 1981, n. 416, Disciplina delle imprese editrici e provvidenze per l'editoria), il cui scopo principale è quello di dare trasparenza agli assetti proprietari degli operatori nei settori dell'editoria e della radiotelevisione. L'attestazione da parte del Registro sul controllo (di diritto e di fatto, *ex* art. 2359 c.c.) è richiesta nell'ambito del rilascio delle provvidenze all'editoria erogate dal Dipartimento per l'informazione e l'editoria della Presidenza del Consiglio (l. n. 250/1990 e, da ultimo, d.P.R. n. 223/2010), nel rilascio dei titoli autorizzatori ai fornitori di servizi *media* da parte del MiSE (l. n. 177/2005) e nell'accesso alle provvidenze per le emittenti locali gestite dai Co.Re.Com (l. n. 448/1998).

Al riguardo, l'Ufficio ha evidenziato che, per quanto riguarda la possibilità di verificare i dati anagrafici dei soggetti non camerali e dei loro amministratori mediante un collegamento telematico con l'Agenzia delle entrate, in parallelo a quello attivato, correttamente, con le Camere di commercio per i soggetti camerali, il d.P.R. 10 febbraio 2000, n. 361 (Regolamento per la semplificazione dei procedimenti di riconoscimento di persone giuridiche private in attuazione delle prescrizioni della legge 15 marzo 1997, n. 59) ha istituito il Registro delle persone giuridiche presso le prefetture (ovvero le regioni o le province autonome competenti), nel quale, in analogia con quanto previsto per il Registro delle imprese tenuto dalla Camera di commercio, sono indicati l'atto costitutivo, la denominazione, lo scopo, il patrimonio, la durata, qualora sia stata determinata, la sede della persona giuridica e il cognome, il nome e il codice fiscale degli amministratori, con menzione di quelli ai quali è attribuita la rappresentanza (artt. 3 e 4). Il Registro e i documenti delle persone giuridiche sono consultabili da chiunque (art. 3, comma 8) e tale forma di pubblicità si estende alle modificazioni dell'atto costitutivo e dello statuto, alle deliberazioni di scioglimento, ai provvedimenti che ordinano lo scioglimento o accertano l'estinzione, al cognome e nome dei liquidatori e a tutti gli altri atti e fatti la cui iscrizione è espressamente prevista da norme di legge o di regolamento (art. 4). È inoltre previsto che le prefetture e le regioni provvedano ad attivare collegamenti telematici per lo scambio dei dati e delle informazioni (art. 1) e che agli adempimenti previsti dal regolamento è data attuazione mediante l'utilizzo dei mezzi telematici previsti dalle norme vigenti (art. 3).

In tale quadro è stato evidenziato che le funzioni di controllo previste dal regolamento Agcom (art. 16, comma 1, All. A alla delibera n. 666/08/CONS del 26 novembre 2008, Regolamento per l'organizzazione e la tenuta del Registro degli operatori di comunicazione) sulle dichiarazioni rese dai legali rappresentanti dei soggetti iscritti al Registro degli operatori di comunicazione, potrebbero utilmente essere effettuate mediante l'accesso telematico al Registro delle persone giuridiche, che è per legge la banca dati dove le informazioni di interesse devono essere iscritte ed aggiornate (nota 5 settembre 2014).

L'Ufficio territoriale del governo di Gorizia ha interpellato il Garante in ordine alla possibilità di trasmettere ad un Comando militare dell'esercito copia di un'ordinanza-ingiunzione (violazione dell'art. 688 c.p., depenalizzato con d.lgs. n. 507/1999) adottata dalla medesima Prefettura nei confronti di un militare in servizio presso il predetto Comando, avanti al quale pendeva una inchiesta formale per la verifica di eventuali responsabilità anche di natura disciplinare. A tal proposito, richiamate le indicazioni fornite con 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 (doc. web n. 1417809), è stato ricordato che la comunicazione di dati personali da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento (art. 19, comma 2, del Codice) e che spetta all'amministrazione interessata verificare il quadro normativo di riferimento, nonché quello di settore, relativo all'amministrazione richiedente le informazioni (nota 21 gennaio 2014).

L'Asl Roma E ha interpellato l'Autorità, ai sensi degli artt. 19, comma 2, e 39 del Codice, al fine di consentire ad un Comando di polizia municipale di Roma Capitale l'accesso alle banche dati aziendali per verificare se la residenza/domicilio, dichiarata all'azienda dagli utenti, risulti diversa da quella ufficiale, e poter così effettuare la notifica di atti a quei soggetti che, all'indirizzo risultante all'anagrafe del Comune di Roma, risultano spesso trasferiti, sconosciuti o irreperibili. L'Ufficio ha rappresentato che il Codice consente, in via residuale, che le amministrazioni pub-

bliche possano comunicare ad altri soggetti pubblici dati personali non sensibili, ove tale comunicazione, benché non prevista da una norma di legge o di regolamento, sia necessaria per lo svolgimento di funzioni istituzionali dell'amministrazione richiedente, verificando anche che tali finalità non possano essere altrimenti perseguite senza l'utilizzo dei dati oggetto della richiesta (cfr. artt. 18, comma, 2, 19, comma 2 e 39, del Codice). In relazione alla fattispecie considerata, è stato evidenziato che gli artt. 137 e ss. c.p.c. e 148 e ss. c.p.p. disciplinano puntualmente le modalità di notifica degli atti, comprese le ipotesi di irreperibilità del destinatario dell'atto, e che pertanto non risultava comprovata l'esigenza di acquisire tali informazioni per il perseguimento delle finalità di notifica degli atti (nota 3 aprile 2014).

Nella materia considerata l'Ufficio ha più volte precisato che nella comunicazione effettuata al Garante ai sensi degli artt. 19, comma 2, e 39, del Codice il titolare deve evidenziare motivatamente l'effettiva necessità dei dati richiesti per lo svolgimento di finalità attinenti alle funzioni istituzionali dell'amministrazione istante, che non potrebbero essere comunque perseguite con modalità che non prevedano il trattamento di dati personali.

In tale quadro, il Ministero dell'istruzione, dell'università e della ricerca ha effettuato una comunicazione al Garante al fine di trasmettere ad un'università, che ne aveva fatto richiesta, alcuni dati personali riferiti agli "alunni frequentanti il secondo anno delle scuole secondarie di secondo grado della provincia di Palermo, per l'anno scolastico 2013/2014". L'università, in particolare, richiedeva i seguenti dati personali (riferiti per lo più a minori): istituto con destinazione per plessi; sezione di frequenza; genere; anno di nascita; nazionalità; indirizzo. Tale richiesta è stata avanzata per la realizzazione di un progetto di ricerca scientifico volto ad investigare i processi di accumulazione del cd. "capitale civico" ed i suoi riflessi sul "capitale umano" nonché a verificare "la trasmissione intergenerazionale dei valori civici ed il ruolo del contesto di riferimento in cui avviene il processo di trasmissione". A tal fine, acquisita la disponibilità dell'istituto scolastico, gli alunni sarebbero stati intervistati con l'autorizzazione degli esercenti la potestà genitoriale. Al riguardo, tenuto anche conto della minore età degli interessati, non è stata rilevata la sussistenza dei presupposti per attivare il flusso di dati sopra descritto (artt. 19, comma 2 e 39 del Codice). Ciò in quanto non risultava evidenziata l'effettiva indispensabilità, rispetto alla finalità che l'università intendeva perseguire, di raccogliere i predetti dati personali presso un soggetto terzo. La ricerca, infatti, ben avrebbe potuto essere perseguita con modalità tali da consentire la raccolta diretta delle informazioni presso gli interessati, previa idonea informativa e attestazione della volontarietà di parteciparvi. L'Ufficio ha rilevato, inoltre, che non risultava garantita la volontarietà dell'adesione degli interessati alla ricerca, eventualmente attraverso i soggetti esercenti la potestà genitoriale, né prevista la preventiva informativa sul trattamento dei dati personali (di cui agli artt. 13 del Codice e 6 del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, All. A.4 al Codice). Non sono risultate, inoltre, evidenziate le modalità con le quali l'università avrebbe trattato le informazioni personali raccolte presso il Ministero e relative agli studenti non aderenti all'iniziativa (nota 30 aprile 2014).

5 La pubblicazione delle sentenze nei siti delle autorità giurisdizionali

La pubblicazione dei dati in rete cambia profondamente l'informazione nel significato, nel fine, nel valore, ma anche nei rischi. Ciò vale anche per l'informazione giuridica e, in particolare, per la pubblicazione delle sentenze nel sito della Corte di Cassazione, avviata nel 2014, e nel nuovo sito della Giustizia amministrativa. Al riguardo il Garante – anche con una lettera del 6 ottobre 2014 indirizzata al Primo Presidente della Corte di Cassazione (cfr. doc. web n. 3432529) – ha rappresentato, in contatti con gli uffici della stessa Corte, poi anche con il Consiglio Superiore della Magistratura, per quanto riguarda la giurisdizione ordinaria, e con il segretariato generale della Giustizia amministrativa, che la natura pubblica della sentenza e del processo non implica che siano perciò solo conoscibili da chiunque, tramite il web, le generalità degli interessati con tutti i dettagli delle loro personali vicende, spesso delicati anche quando non si riferiscano a minori, ovvero a dati giudiziari o sensibili. Questo anche in considerazione dei rischi di indicizzazione, decontestualizzazione, se non di alterazione dei dati stessi, inevitabilmente connessi alla loro indiscriminata accessibilità via web, rischi ben evidenziati dalla sentenza della Corte di giustizia dell'Unione europea del 13 maggio 2014, C-131-12, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González (doc. web n. 3127044).

Si tratta di profili complessi anche nelle implicazioni di carattere ordinamentale, che sono tuttora oggetto di approfondimento e di confronto in spirito di collaborazione istituzionale, nell'intendimento di giungere ad una soluzione condivisa, rispettosa delle esigenze di protezione dei dati personali degli interessati.

6 La sanità

6.1. *I trattamenti per finalità di cura*

In relazione al trattamento dei dati personali dei pazienti ai fini di prevenzione, diagnosi, cura e riabilitazione degli stessi, è stata definita l'istruttoria di segnalazioni relative alla prassi, seguita da molti ospedali, di somministrare sistematicamente ai pazienti, all'atto del ricovero, un questionario nel quale erano formulati quesiti sul credo professato. Con un provvedimento generale (12 novembre 2014, n. 515, doc. web n. 3624070) il Garante ha precisato che le strutture sanitarie non possono raccogliere in maniera sistematica e preventiva informazioni sulle convinzioni religiose dei pazienti. Tali informazioni possono essere trattate solo se il malato richieda di usufruire dell'assistenza religiosa e spirituale (bisogno di conforto o di sacramento al letto) o se ciò risulti indispensabile nello svolgimento dei servizi necroscopici per rispettare le volontà espresse in vita dal paziente. Le richieste di assistenza religiosa e spirituale possono essere comunicate verbalmente dal paziente, da un familiare o un convivente, al personale di reparto, che provvederà a trasmetterle alla direzione sanitaria. Anche la volontà di non sottoporsi ad alcuni trattamenti terapeutici (ad es., rifiuto alle trasfusioni) o la preferenza per un determinato regime alimentare deve poter essere espressa senza dover enunciare le eventuali motivazioni di natura religiosa che ne sono alla base (non essendo tale informazione indispensabile).

In ordine al trattamento dei dati personali effettuato dai medici di medicina generale (mmg) e dai pediatri di libera scelta (pls), il Presidente dell'Autorità ha inviato una lettera al Presidente della Federazione italiana medici di medicina generale (Fimmg) per sgombrare il campo da allarmi ingiustificati (diffusisi a seguito di articoli e lettere dei lettori apparsi su alcuni quotidiani nazionali) su presunti divieti per tale categoria di professionisti che sarebbero stati imposti dell'Autorità (nota 12 novembre 2014, doc. web n. 3533561). In tale nota si è ricordato che i mmg/pls, in qualità di titolari del trattamento, devono adottare idonei accorgimenti per garantire – anche nell'organizzazione delle modalità di consegna di certificati e ricette – il rispetto del diritto alla riservatezza del paziente osservando le misure che il Codice prescrive in ambito sanitario; si è altresì chiarito che prescrizioni e certificati medici possono essere ritirati anche da persone diverse dai diretti interessati, purché in base a una delega scritta da parte del paziente e mediante la consegna degli stessi in busta chiusa.

In relazione all'invio a diversi soggetti istituzionali da parte di una residenza per anziani di una *e-mail*, contenente numerosi dati sanitari dei propri ospiti, al fine di evidenziare i danni che gli stessi avrebbero ricevuto da un eventuale trasferimento di sede, l'Ufficio ha ritenuto che tali rimostranze sarebbero potute avvenire con modalità più rispettose della riservatezza dei ricoverati considerando tale comunicazione di dati sensibili effettuata in assenza di un presupposto legittimante; sul caso è stato avviato un procedimento sanzionatorio (nota 6 marzo 2014).

Attività istruttorie sono state svolte in merito al trattamento dei dati personali effettuato in fase di prenotazione delle prestazioni sanitarie, prestando particolare attenzione alle attività poste in essere al riguardo dai centri unici di prenotazione (cup) e dalle farmacie convenzionate con le strutture sanitarie.

Specifici interventi sono stati posti in essere anche con riferimento alle modalità con le quali le strutture sanitarie custodiscono gli atti e i documenti sanitari cartacei. In alcuni casi tali accertamenti hanno portato all'avvio di un procedimento sanzionatorio per mancata adozione delle misure di sicurezza con riferimento all'individuazione delle modalità tecniche volte ad assicurare che l'accesso agli archivi sanitari sia selezionato e controllato (note 13 gennaio, 28 marzo e 2 aprile 2014).

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

Continuano a pervenire numerose segnalazioni in merito ai modelli di informativa e di consenso utilizzati dalle strutture sanitarie con riferimento al trattamento dei dati personali ai fini di cura.

A seguito dell'intervento dell'Ufficio una Asl ha modificato il modello di informativa in uso con i propri pazienti evidenziando meglio i trattamenti di dati personali effettuati per fini di cura e quelli svolti per attività di ricerca e per finalità di carattere amministrativo. L'Azienda ha poi provveduto ad integrare l'informativa con l'indicazione dei soggetti cui possono essere comunicati i dati personali e delle conseguenze in caso di mancato conferimento del consenso dell'interessato (nota 17 luglio 2014). L'inidoneità dell'informativa precedentemente resa ai pazienti ha portato all'avvio di un procedimento sanzionatorio.

Anche in altri casi strutture ospedaliere e singoli professionisti sanitari hanno provveduto a rivedere le procedure di raccolta del consenso ai trattamenti dei dati personali dei pazienti nonché i modelli di informativa utilizzati, con particolare riferimento agli episodi di ricovero.

Una significativa attività istruttoria è stata avviata dall'Ufficio a seguito di una segnalazione in cui una donatrice di sangue evidenziava la scarsa chiarezza dell'informativa fornita all'atto della donazione. In fase istruttoria si è appreso che tale modello di informativa era in uso presso tutti i centri trasfusionali e che era stato adottato sulla base di un decreto del Ministero della salute emanato senza il preventivo parere del Garante (d.m. 3 marzo 2005). È stato quindi avviato un tavolo di lavoro con il Ministero della salute al fine di individuare un nuovo modello di informativa per i trattamenti di dati personali connessi all'attività di donazione del sangue. Tale modello sarà allegato al decreto ministeriale di prossima emanazione in materia di donazione di sangue e di emocomponenti, da adottarsi previo parere del Garante. Il nuovo modello di informativa supera le criticità precedentemente riscontrate evidenziando meglio le modalità e finalità del trattamento di dati personali e l'ambito di comunicazione degli stessi.

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

Fse

L'Autorità ha confermato il suo ruolo di primario attore istituzionale nell'implementazione del Fascicolo sanitario elettronico (Fse) secondo canoni conformi ai principi che governano la protezione dei dati personali (ed in merito al quale v. già le "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di *dossier* sanitario", provv. 16 luglio 2009, n. 25, doc. web n. 1634116). Dal punto di vista normativo, il Fse è stato disciplinato dall'art. 12, d.l. 18 ottobre 2012, n. 179 (convertito dalla l. 17 dicembre 2012, n. 221), successivamente modificato dal d.l. 21 giugno 2013, n. 69 (a sua volta convertito dalla l. 9 agosto 2013, n. 98), disposizione quest'ultima che ha previsto, tra l'altro, l'adozione di una serie di decreti attuativi volti a consentire il concreto avvio della realizzazione del Fascicolo.

Come già descritto nella Relazione 2013, l'Autorità ha partecipato all'apposito tavolo di lavoro istituito presso il Ministero della salute, contribuendo alla stesura del primo dei regolamenti previsti. Le indicazioni fornite hanno riguardato, in par-

ticolare: la richiesta di uno specifico consenso in relazione al trattamento di informazioni particolarmente delicate (come quelle concernenti la sieropositività, l'interruzione volontaria di gravidanza, la violenza sessuale, la pedofilia, l'uso di sostanze stupefacenti, il parto in anonimato); una più netta distinzione fra consenso all'alimentazione e consenso alla consultazione del Fse per finalità di cura; l'oscuramento dell'oscuramento; la previsione di accesso al Fse solo da parte del personale che abbia effettivamente in cura il paziente e per il tempo a ciò necessario; l'introduzione di un meccanismo di avviso tempestivo del Garante in caso di cd. *data breach*.

In occasione del medesimo tavolo di lavoro l'Autorità ha altresì posto il problema causato dalla revisione dell'art. 12, d.l. 18 ottobre 2012, n. 179 ad opera del d.l. 21 giugno 2013, n. 69, già segnalato al Parlamento al momento della conversione. La novella legislativa prevede per le regioni e i ministeri coinvolti la possibilità di accedere ad un'ampia gamma di dati (come le risultanze diagnostiche radiologiche o gli esiti di analisi cliniche) sia per finalità di ricerca che per finalità di governo. Tale possibilità è stata ritenuta dal Garante sproporzionata in relazione ai predetti scopi. In fase attuativa della richiamata norma di legge gli attori istituzionali hanno raccolto il monito dell'Autorità, prevedendo nel primo dei decreti di attuazione del Fse di escludere espressamente l'accesso alla documentazione diagnostica, quali le copie per immagine di documenti analogici e le informazioni grafiche non strutturate, per finalità di governo. In considerazione dell'accoglimento di tutte le indicazioni rese dall'Autorità, il Garante ha potuto così esprimere parere favorevole sullo schema di decreto (parere 22 maggio 2014, n. 261, doc. web n. 3230826).

Dossier sanitario

Sul versante del *dossier* sanitario, data la vasta diffusione di tale strumento sul territorio nazionale e le diverse segnalazioni ricevute, si sono resi necessari numerosi interventi da parte dell'Autorità volti a verificare se i sistemi in uso rispettassero le misure indicate dal Garante nelle citate Linee guida. In proposito, si ricorda che il *dossier* sanitario viene costituito presso un organismo sanitario in qualità di unico titolare del trattamento al cui interno operino più professionisti (ad es., ospedale o azienda sanitaria) e contiene informazioni inerenti allo stato di salute di un individuo relative ad eventi clinici presenti e trascorsi (ad es., referti, documentazione relativa a ricoveri, accessi al pronto soccorso) volte a documentarne la storia clinica. Le istruttorie, alcune delle quali tuttora in corso, sono state effettuate anche mediante specifici accertamenti ispettivi e hanno riguardato pure strutture sanitarie di tipo universitario.

Come si è già dato ampiamente conto nella Relazione 2013 (p. 69), un primo intervento sul *dossier* sanitario è stato effettuato nei confronti di tutte le strutture sanitarie pubbliche della Regione Friuli-Venezia Giulia (provv. 10 gennaio 2013, n. 3, doc. web n. 2284708). In relazione a questa vicenda è stato definito un ulteriore procedimento istruttorio, riferito a fatti anteriori al citato provvedimento, ove è stato accertato un accesso abusivo ai dati personali contenuti nel *dossier* del segnalante da parte di personale medico privo di alcun titolo legittimante; tale riscontro ha comportato altresì l'avvio di un apposito procedimento sanzionatorio (nota 14 febbraio 2014).

Merita evidenziare che al termine di specifiche attività istruttorie l'Autorità ha adottato tre provvedimenti inibitori e prescrittivi nei confronti di strutture sanitarie pubbliche anche di rilievo universitario.

La prima di queste strutture chiamata a fornire spiegazioni rispetto alle criticità inizialmente emerse in sede di giustizia contabile è stata l'Azienda sanitaria dell'Alto Adige (provv. 3 luglio 2014, n. 340, doc. web n. 3325808); la vicenda, infatti, è scaturita da una segnalazione della Procura regionale della Corte dei conti territorialmente competente nella quale si dava notizia della condanna di una dipendente

dell'Azienda per il reato di cui all'art. 326 del c.p., in quanto la stessa, abusando del proprio incarico, aveva rivelato (in più occasioni e a più dipendenti) lo stato di sieropositività di una collega. Gli aspetti di criticità rilevati dall'Autorità hanno riguardato la mancata acquisizione del consenso informato dei pazienti alla costituzione del *dossier* sanitario e la possibilità per qualsiasi operatore sanitario di accedere al *dossier* a prescindere dalla circostanza della presa in carico dell'interessato. Il Garante ha prescritto all'Azienda di raccogliere il consenso informato degli interessati anche con riferimento agli eventi clinici pregressi nonché in relazione alla (eventuale) volontà di oscurare talune informazioni mediche; inoltre, in attesa di acquisire tale consenso, è stato imposto di circoscrivere l'accesso ai *dossier* sanitari ai soli professionisti che avessero effettivamente in cura gli interessati, peraltro per il solo periodo di tempo in cui è articolato il percorso di cura. L'Azienda nel corso del procedimento ha fornito rassicurazioni sulla circostanza di aver avviato un processo di adeguamento alle indicazioni fornite a suo tempo nelle Linee guida del Garante. In ragione della complessità ed eterogeneità dei sistemi informativi in uso presso i comprensori territoriali di cui l'Azienda è composta, il Garante ha successivamente concesso una proroga per l'adeguamento di alcune delle misure prescritte (provv. 11 settembre 2014, n. 403, doc. web n. 3494478).

Il secondo intervento prescrittivo del 2014 in tema di *dossier* sanitario si è rivolto all'Azienda ospedaliero universitaria S. Orsola Malpighi di Bologna, nei confronti della quale l'Ufficio aveva ricevuto alcune segnalazioni aventi ad oggetto la possibilità per ogni medico di accedere ai referti di chiunque vi avesse effettuato un esame clinico (provv. 23 ottobre 2014, n. 468, doc. web n. 3570631). In questo caso l'Azienda, già all'indomani degli accertamenti ispettivi, ha avviato un processo di riorganizzazione complessivo sul sistema di trattamento dei dati personali effettuato con lo strumento del *dossier* sanitario, impegnandosi a completare l'adozione di tutti gli accorgimenti richiesti entro marzo 2015. La peculiarità di questo provvedimento rispetto ai precedenti è la misura con cui si è obbligata l'Azienda ad acquisire uno specifico consenso informato per l'utilizzo di informazioni particolarmente delicate quali quelle relative alle prestazioni erogate a seguito di atti di violenza sessuale o di pedofilia, oppure in occasione dell'accertamento dello stato di sieropositività, dell'uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, o ancora in occasione degli interventi di interruzione volontaria della gravidanza o relativi al parto in anonimato, nonché con riferimento ai servizi offerti dai consultori familiari. Questo provvedimento è stato altresì inviato alla Regione Emilia Romagna affinché provveda a sensibilizzare tutte le altre aziende afferenti al Servizio sanitario regionale sulle cautele da adottare in caso di costituzione del *dossier* sanitario.

Infine, il Garante si è pronunciato nei confronti dell'Azienda Policlinico Umberto I di Roma, a seguito di una vicenda originata, oltre che da alcune segnalazioni, dall'invio a quotidiani nazionali ed istituzioni di una lettera anonima contenente dati idonei a rivelare lo stato di salute estrapolati dai rapporti di pronto soccorso del Policlinico e riferiti a numerosi pazienti (provv. 18 dicembre 2014, n. 610, doc. web n. 3725976). In questo caso le precisazioni formulate dalla direzione del Policlinico hanno evidenziato, a differenza dei citati precedenti, l'effettiva esistenza di limiti all'accesso al *dossier* al solo personale sanitario che avesse in cura ciascun paziente: l'Autorità ha quindi preso atto di quanto affermato e si è riservata di valutare le modalità attraverso le quali tale garanzia è stata realizzata nei sistemi informativi in uso. Per quanto riguarda il consenso informato al trattamento mediante *dossier* sanitario, a seguito degli accertamenti ispettivi l'Azienda ha predisposto nuovi modelli, ma la persistenza di alcune criticità (ad es. sulla cd. gestione del pregresso o sulle informazioni di particolare delicatezza, quali quelle concernenti la sie-

ropositività o l'interruzione volontaria di gravidanza) ha indotto il Garante a prescrivere apposite misure correttive. Dell'adozione di questi accorgimenti, come anche del completamento di quelli già avviati spontaneamente, il Policlinico è tenuto a dare riscontro all'Autorità entro i primi mesi del 2015.

Anche in questa vicenda, al pari di quella descritta precedentemente sull'Azienda bolognese, è stato deciso di informare le autorità regionali, al fine di promuovere in tutto il Servizio sanitario laziale una corretta implementazione del *dossier* sanitario.

6.1.3. I referti e la documentazione sanitaria

Sono continuate a pervenire segnalazioni in ordine alle modalità con le quali strutture sanitarie e singoli professionisti consegnano referti e altra documentazione medica ai pazienti o a soggetti delegati, in busta aperta. A seguito degli interventi dell'Ufficio, le strutture sanitarie coinvolte, laddove tali episodi non potessero essere ricondotti a circostanze fortuite, hanno provveduto a modificare i processi individuati per la consegna della documentazione sanitaria a soggetti diversi dall'interessato e a prevedere una attività di formazione per il personale a ciò incaricato (cfr., ad es., note 9 aprile e 29 dicembre 2014). In altri casi, alcuni pazienti hanno segnalato al Garante di aver ricevuto da parte di ospedali e Asl documentazione sanitaria riferita a terzi. In tali casi, l'Autorità ha avviato dei procedimenti sanzionatori per la comunicazione di dati sanitari a soggetti non legittimati ed ha vigilato in merito alla revisione delle procedure per la consegna dei referti affinché siano più rispettose del quadro normativo vigente (cfr., ad es., nota 17 luglio 2014).

Merita particolare attenzione quanto segnalato su tale problematica da un paziente che aveva visto consegnare il referto relativo ad un esame ematico (eseguito spontaneamente) al proprio datore di lavoro. Essendo tale comunicazione di dati sanitari avvenuta al di fuori delle procedure e dei limiti previsti dalla normativa vigente per la verifica della persistente idoneità al servizio, è stato avviato un procedimento sanzionatorio per l'indebita comunicazione di dati sanitari a terzi nonché disposti ulteriori accertamenti in merito al trattamento dei dati effettuato dal datore di lavoro (nota 15 aprile 2014).

Con riferimento ai servizi di pagamento del *ticket* e di ritiro dei referti offerti da Poste italiane, l'Autorità ha concluso l'istruttoria avviata nel 2013 – anche mediante accertamenti ispettivi – adottando un provvedimento prescrittivo nei confronti dell'Azienda sanitaria di Firenze (provv. 13 marzo 2014, n. 120, doc. web n. 3041470).

Dagli accertamenti svolti erano emerse, infatti, serie criticità sulle procedure adottate, specie con riferimento alle modalità di identificazione degli utenti. Né il servizio di pagamento offerto dalla società attraverso il proprio sito, né quello erogato tramite lo sportello postale garantiva infatti che le informazioni sulla salute, contenute nelle fatture rilasciate all'atto del pagamento, fossero fornite esclusivamente al diretto interessato o alla persona da lui delegata. Il servizio *online*, in particolare, consentiva a chiunque, in possesso del codice fiscale di una persona che avesse prenotato una prestazione sanitaria, di accedere a informazioni personali e, nel caso di pagamento del *ticket*, di conoscere anche il tipo di prestazione sanitaria richiesta (ad es., visita chemioterapica, radioterapia, ecc.). Il Garante ha pertanto prescritto all'Azienda di introdurre un sistema di identificazione, modificando la "maschera" di accesso al servizio di pagamento *online* con l'introduzione di un apposito campo che consente all'utente di inserire il codice fiscale e il codice di prenotazione cup. Analogamente l'operatore dello sportello postale, prima di erogare il servizio, dovrà verificare l'identità di chi effettua il pagamento del *ticket*, controllando un documento di riconoscimento e annotandone gli estremi. Nel caso in cui allo sportello si presenti una persona diversa dal beneficiario della prestazione, l'operatore dovrà con-

segnare la fattura in busta chiusa o spillata, dopo aver verificato che il delegato sia in possesso del codice fiscale del diretto interessato e del codice di prenotazione rilasciato dal Cup. Secondo quanto prescritto dal Garante, all'azienda sanitaria spetta inoltre il compito di verificare che Poste italiane fornisca idonee istruzioni ai propri impiegati e di effettuare controlli a campione sul rispetto delle suddette procedure.

Scambio di embrioni

L'Autorità ha prestato una particolare attenzione nei confronti del trattamento di dati personali avvenuto nell'ambito della nota vicenda sullo scambio di embrioni all'ospedale Pertini di Roma, in quanto tale evento coinvolgeva sia aspetti sostanziali della dignità e dell'identità personale sia la tutela dei diritti fondamentali dei soggetti giuridici coinvolti. Considerato il contesto del trattamento, il Garante ha ritenuto che i dati personali relativi all'identità della gestante dovessero essere reputati idonei a rivelarne lo stato di salute. L'Autorità ha poi ricordato che spetta alla struttura sanitaria, destinataria della richiesta di accesso a tali dati, consentire o negare l'accesso agli stessi, verificando, nel caso concreto, la configurabilità in capo all'istante di una situazione giuridica di rango almeno pari ai diritti dell'interessato ovvero consistente in un diritto della personalità o in altro diritto o libertà fondamentale e inviolabile (art. 60 del Codice). Tale bilanciamento deve tener conto delle ragioni a fondamento della richiesta di accesso degli istanti e dell'eventuale rifiuto opposto dall'altra coppia, nonché della tutela dei diritti e degli interessi dei nascituri (nota 23 maggio 2014).

6.1.4. La tutela della dignità della persona

Anonimato della madre e diritto a conoscere le proprie origini

Particolare attenzione è stata prestata al trattamento dei dati personali delle donne che decidono di partorire in anonimato, con specifico riferimento alla tutela della loro dignità e riservatezza (art. 30, comma 1, d.P.R. n. 396/2000). Come è noto, con la sentenza n. 278/2013 la Corte costituzionale è intervenuta in relazione alla manifestazione di volontà che la partoriente può esprimere in occasione del parto a non essere nominata nella dichiarazione di nascita e sul conseguente limite all'accesso a tali informazioni da parte del figlio biologico (art. 28, l. n. 184/1983). In particolare, la Corte, ritenuto che il *vulnus* di tali disposizioni sia "rappresentato dalla irreversibilità del segreto", ha ritenutoo che il citato art. 28 sia "in contrasto con gli artt. 2 e 3 Cost." e stabilito che "sarà compito del legislatore introdurre apposite disposizioni volte a consentire la verifica della perdurante attualità della scelta della madre naturale di non voler essere nominata e, nello stesso tempo, a cautelare in termini rigorosi il suo diritto all'anonimato, secondo scelte procedimentali che circoscrivano adeguatamente le modalità di accesso, anche da parte degli uffici competenti, ai dati di tipo identificativo, agli effetti della verifica di cui innanzi si è detto". L'illegittimità costituzionale è stata dichiarata con riferimento alla circostanza che il richiamato art. 28, l. n. 184/1983 "non prevede – attraverso un procedimento, stabilito dalla legge, che assicuri la massima riservatezza – la possibilità per il giudice di interpellare la madre – che abbia dichiarato di non voler essere nominata [...] su richiesta del figlio, ai fini di una eventuale revoca di tale dichiarazione".

A seguito di tale sentenza sono state segnalate al Garante iniziative di tribunali che hanno provveduto, con varie modalità, a prendere contatto con la madre della persona che aveva presentato istanza di accesso alle proprie origini biologiche.

Tenendo conto di tali segnalazioni, l'Ufficio ha seguito con particolare attenzione i lavori parlamentari in materia. Contestualmente la Commissione giustizia della Camera dei deputati, la quale sta esaminando – in sede referente – le proposte di legge, ha richiesto al Garante un contributo sul tema. Al riguardo, il Presidente dell'Autorità ha ritenuto opportuno fornire alla Commissione alcune osservazioni con riferimento agli aspetti di protezione dei dati personali che si rinvengono nelle

proposte di legge in corso di esame. Il Presidente ha evidenziato come la sentenza della Corte non abbia scalfito il diritto alla riservatezza delle madri che al momento del parto si sono avvalse del diritto di non essere nominate, non avendo la pronuncia interessato il menzionato art. 30, d.P.R. n. 396/2000 ed avendo, al contrario, la Corte ribadito la necessità di proteggere in termini rigorosi il diritto all'anonimato delle donne "attraverso un procedimento, stabilito dalla legge, che assicuri la massima riservatezza" delle stesse.

Con riferimento ai casi segnalati, in cui l'autorità giudiziaria ha dato immediata applicazione alla sentenza della Corte costituzionale – consentendo ai figli di rintracciare le madri naturali anche nel caso in cui queste donne avessero all'epoca esercitato la facoltà di non essere nominate nella dichiarazione di nascita –, il Presidente dell'Autorità ha evidenziato che i rischi connessi ad una "flessibilizzazione" della garanzia dell'anonimato della madre naturale in assenza di adeguati supporti normativi che ne definiscano modalità e procedure sono già concreti e solo un organico intervento del legislatore può assicurare che il diritto dei figli a conoscere le proprie origini biologiche non vada a completo detrimento della riservatezza delle donne. Si è ha pertanto ravvisata la necessità di effettuare un corretto bilanciamento tra la tutela rigorosa dell'anonimato della donna e il diritto del figlio a conoscere le proprie origini attraverso l'individuazione di procedure tali da consentire al figlio di avanzare la richiesta di conoscere l'identità della madre e, ove il legislatore lo ritenga, la possibilità per la donna di rinunciare preventivamente all'anonimato a prescindere dall'istanza del figlio. Il Presidente ha, quindi, sollecitato il legislatore a introdurre una procedura che consenta l'eventuale incontro di queste due volontà (quella del figlio di avvicinarsi alla madre e quella di costei di rivedere la propria scelta passata), garantendo la massima riservatezza di ciascuno, e ha evidenziato che tale procedura si potrebbe incardinare in capo ad una autorità indipendente.

Presìdi sanitari

A seguito dell'adozione del provvedimento del 2013 sulle modalità di consegna dei presìdi sanitari agli interessati da parte delle aziende sanitarie e delle ditte aggiudicatarie (provv. 21 novembre 2013, n. 520, doc. web n. 2803050), le strutture sanitarie hanno rivisto i propri processi organizzativi. In particolare, sono state riviste le modalità di consegna dei suddetti presìdi a soggetti diversi dall'interessato, previa delega di quest'ultimo, nonché fornite precise istruzioni al personale addetto alla distribuzione in merito all'adozione di idonee misure atte a garantire che terzi, quali ad esempio i vicini di casa, possano venire a conoscenza – anche indirettamente – della circostanza che l'interessato necessita di specifici presìdi sanitari e che, quindi, possa essere lesa la dignità e la riservatezza di quest'ultimo (v., ad es., nota 3 aprile 2014).

Distanze di cortesia e modulistica

Continuano a pervenire numerose segnalazioni in ordine al mancato rispetto delle misure poste a tutela della riservatezza da parte delle aziende sanitarie con riferimento alle attività di prenotazione di esami clinici, di raccolta dell'anamnesi e di erogazione delle prestazioni sanitarie. In tali occasioni le strutture sanitarie sono state richiamate al rispetto delle misure individuate dal Codice e dallo stesso Garante già in passato (provv. 9 novembre 2005, doc. web n. 1191411). In particolare è stata richiamata la necessità di predisporre apposite distanze di cortesia in tutti i casi in cui si effettua un trattamento di dati sanitari (ad es., operazioni di sportello), nel rispetto dei canoni di confidenzialità e riservatezza dell'interessato, nonché di porre particolare attenzione al rispetto della dignità dei pazienti sottoposti a trattamenti medici invasivi (note 9 e 24 aprile 2014, 21, 23 ottobre e 21 novembre 2014).

L'Autorità è anche intervenuta in un caso in cui un ospedale universitario utilizzava modelli per giustificare le assenza dal lavoro dei pazienti in cui era indicato il reparto ove questi si erano recati, con la conseguente modifica della modulistica che

ha portato all'eliminazione dell'indicazione del reparto e di ogni altra indicazione da cui si potesse desumere lo stato di salute del paziente (correlandone l'identità con la specifica struttura sanitaria visitata).

In un altro caso è stato lamentato che un ospedale, presso il quale era stato curato l'interessato, aveva trasmesso la denuncia di malattia infettiva al comune di residenza anziché alla Asl territorialmente competente come prevede la normativa sulle malattie infettive e diffusive di cui al d.m. 15 dicembre 1990. Dagli approfondimenti svolti è emerso che la segnalazione era stata recapitata al comune di residenza dell'interessato a causa dell'imprecisa indicazione dell'ente destinatario della comunicazione nella busta contenente la segnalazione. A seguito dell'intervento dell'Ufficio l'ospedale ha rivisto e modificato le procedure utilizzate per la trasmissione delle schede di notifica delle malattie infettive. In particolare sono state fornite indicazioni agli uffici affinché nelle buste contenenti le segnalazioni riguardanti le malattie infettive sia riportato l'indirizzo completo dell'autorità sanitaria competente insieme all'indicazione relativa alla particolare delicatezza dei dati sanitari ivi contenuti (nota 17 febbraio 2015).

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

L'Autorità ha mantenuto una costante attenzione in merito alla questione relativa al rilascio del codice di esenzione dalla partecipazione al costo per le prestazioni di assistenza sanitaria previsto per le infezioni da HIV. La problematica, all'esame dell'Autorità già dal 2013, attiene all'individuazione di idonee cautele volte a non far evincere in modo immediato l'esistenza di un'infezione da HIV attraverso la mera presentazione della documentazione amministrativa necessaria all'erogazione della prestazione sanitaria da parte del Ssn. L'Autorità ha informato al riguardo il Ministero della salute e l'Istituto Superiore di Sanità sull'esperienza maturata sul punto dalla Regione Toscana, al fine di promuovere l'adozione di iniziative organizzative volte ad introdurre procedure per il riconoscimento dell'esenzione più rispettose della riservatezza dei soggetti interessati. La collaborazione istituzionale avviata in tal senso prevede allo stato anche il coinvolgimento delle istituzioni locali competenti (note 5 marzo e 29 dicembre 2014).

Con specifico riferimento ai trattamenti di dati sanitari idonei a rivelare lo stato di sieropositività effettuati a fini di cura dell'interessato l'Autorità è intervenuta in un caso in cui un infermiere, operante presso il reparto di chirurgia di un ospedale lombardo, aveva lasciato incustodita la cartella clinica del segnalante nella stanza di degenza dello stesso. A seguito di tale comportamento, la madre dell'interessato ha appreso lo stato di sieropositività del figlio, il quale aveva espressamente rappresentato al personale medico e infermieristico di non voler far conoscere tale sua situazione ai propri congiunti. Nell'ambito dell'istruttoria, l'Ufficio ha ricordato che la tenuta della cartella clinica configura un trattamento dei dati personali idonei a rivelare lo stato di salute effettuato senza l'ausilio di strumenti elettronici, in relazione al quale devono essere previste procedure per un'idonea custodia degli atti e dei documenti ivi contenuti (art. 35, comma 1, lett. *b*), del Codice). La struttura sanitaria avrebbe dovuto adottare modalità tecniche volte ad assicurare che la cartella clinica, affidata all'incaricato del trattamento per lo svolgimento dei relativi compiti, fosse custodita dagli incaricati fino alla sua restituzione (regola n. 28 del Disciplinare tecnico in materia di misure minime di sicurezza, All. B al Codice). Peraltro, con riferimento alle informazioni relative alla sieropositività, puntuali disposizioni normative impongono l'obbligo per gli operatori sanitari che nell'esercizio della professione ne vengano a conoscenza di "adottare tutte le misure occorrenti per la tutela della riservatezza" (art. 5, l. n. 135/1990). L'Autorità ha poi ricordato che la Corte di Cassazione

(30 gennaio 2009, n. 2468), con riferimento alla custodia nella sala infermieri della cartella clinica relativa ad un malato di Aids, ha precisato che la mera conservazione della cartella in tale locale non è di per sé sufficiente a garantire la riservatezza dei dati personali del paziente anche se tale locale è riservato al personale sanitario, in mancanza di dimostrazione che a detta sala viene effettivamente impedito l'accesso a terzi. In merito alla vicenda è stato quindi avviato un procedimento sanzionatorio relativo al mancato rispetto delle misure minime di sicurezza (artt. 33, 35 e 162 del Codice e regola n. 28 del Disciplinare tecnico) (nota 9 aprile 2014).

6.1.6. Il trattamento di dati sanitari raccolti attraverso apparecchiature diagnostiche

L'Autorità ha svolto approfondimenti in merito al trattamento dei dati personali effettuato tramite apparecchiature di diagnostica per immagini. L'attività istruttoria ha avuto origine da una segnalazione di un'azienda ospedaliera e dai contatti nel frattempo intercorsi con una società che cura la produzione e la distribuzione alle strutture sanitarie di apparecchiature di diagnostica di precisione. La vicenda riguardava le attività di controllo da remoto di questi dispositivi forniti dalla società alle strutture sanitarie, nell'ambito delle quali erano stati impropriamente trasferiti e registrati, sui *server* della capogruppo situati negli Stati Uniti, dati personali eccedenti le finalità di manutenzione delle apparecchiature riferiti ai pazienti, insieme ad altre informazioni relative alle prestazioni delle macchine. Secondo quanto riportato, l'accaduto aveva interessato circa centottanta strutture sanitarie in Italia e più di un milione di pazienti.

Nel corso dei predetti approfondimenti è stato tuttavia riscontrato che, a prescindere dall'incidente di cui era stata data notizia all'Ufficio, le apparecchiature sanitarie per le quali la società fornisce servizi di manutenzione e assistenza erano programmate in modo da connettersi periodicamente e trasmettere automaticamente ai sistemi della società, in condizioni di ordinario funzionamento, flussi di dati sanitari riferiti ai pazienti, sia pure in modo indiretto, quali codici alfanumerici, peso, altezza e informazioni relative agli esami eseguiti. Tali informazioni, ritenute dalla società necessarie per garantire il buon funzionamento e l'affidabilità dei macchinari nonché la prestazione dei relativi servizi, venivano raccolte al di là di quanto previsto nelle clausole contrattuali relative alla fornitura dei servizi alle strutture sanitarie, trasferite verso un Paese il cui ordinamento non assicura un livello di tutela delle persone adeguato senza le necessarie garanzie (artt. 43 e 44 del Codice) e utilizzate per finalità autonomamente individuate dalla società (ad es., ricerca e sviluppo delle apparecchiature e miglioramento della qualità delle stesse).

Di conseguenza l'Autorità ha vietato alla società di proseguire l'ulteriore trattamento non consentito dei dati sanitari riferiti ai pazienti a fini di ricerca e sviluppo delle proprie apparecchiature e di miglioramento della qualità delle stesse, fin tanto che essa non adotti accorgimenti tecnici atti ad anonimizzare efficacemente tali informazioni in modo da non consentire, con l'uso di mezzi ragionevoli, la re-identificazione delle persone cui esse si riferiscono, neanche mediante il ricorso ad altre informazioni nella disponibilità della stessa società, di altre società del gruppo, ovvero di terzi (art. 4, comma 1, lett. *n*), del Codice). Sono state inoltre fornite specifiche prescrizioni alla società volte a precisare nei termini contrattuali e nell'atto di designazione quale responsabile del trattamento le operazioni di trattamento compiute dalla stessa con i dati sanitari dei pazienti raccolti nell'ordinario funzionamento delle apparecchiature.

Per specifici interventi tecnici di manutenzione e di assistenza delle apparecchiature in uso presso le strutture sanitarie (*in loco* e in remoto) che rendono invece indispensabile l'accesso da parte della società ai dati attinenti alla salute dei pazienti

(sia pure indirettamente identificativi), è stato invece richiesto alla società di adottare misure e accorgimenti idonei a proteggere i dati delle persone interessate. In particolare, la società dovrà informare tempestivamente la struttura sanitaria di riferimento dell'intervento eseguito, documentare le operazioni di trattamento effettuate indicando le tipologie di dati coinvolti e le ragioni che hanno reso necessario trattare tali informazioni per assicurare il funzionamento dell'apparecchiatura, registrare le predette operazioni (*access log*) e metterle a disposizione della struttura sanitaria su richiesta, rafforzare le tecniche di pseudonimizzazione dei dati utilizzate in modo da ridurre il rischio di re-identificare gli interessati, nonché effettuare il trasferimento all'estero dei dati dei pazienti nel rispetto delle cautele previste dal Codice.

È stato infine avviato un procedimento sanzionatorio per il trattamento illecito effettuato dalla società (provv. 10 aprile 2014, n. 186, doc. web n. 3152119).

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

L'Autorità ha fornito numerosi chiarimenti ad aziende sanitarie e ad altri soggetti pubblici che istituzionalmente intervengono in ambito sanitario con riferimento ai trattamenti di dati personali effettuati per finalità amministrative correlate alla cura. In particolare, sono state fornite indicazioni in merito a quanto previsto nello schema tipo aggiornato di regolamento per il trattamento dei dati sensibili e giudiziari che possono essere raccolti e utilizzati da regioni, province autonome, aziende sanitarie locali e altre strutture sanitarie facenti parte del Servizio sanitario regionale nell'ambito dello svolgimento delle relative funzioni istituzionali (cfr. ad es., nota 10 e 14 marzo 2014).

L'Autorità ha attivato anche un tavolo di lavoro con l'Agenzia delle entrate in merito alla questione relativa alla presenza di diciture che riportano in modo descrittivo la tipologia dei dispositivi medici e delle prestazioni sanitarie nello scontrino fiscale e nella fattura rilasciati per il relativo acquisto o erogazione. Al riguardo, deve auspicarsi l'individuazione di percorsi per una soluzione idonea a contemperare la protezione dei dati personali idonei a rivelare lo stato di salute degli interessati con le esigenze di escludere che la spesa sostenuta dal contribuente si riferisca a prodotti o prestazioni diverse da quelle effettivamente acquistati o erogate ai fini della detrazione o della deduzione della relativa spesa. L'attività istruttoria dovrà tenere conto anche delle novità legislative in tema di semplificazione fiscale e dichiarazione dei redditi precompilata, con specifico riferimento alle modalità di acquisizione da parte dell'Agenzia delle entrate delle informazioni relative alla prestazioni sanitarie e farmaceutiche usufruite dai contribuenti.

L'Autorità ha inoltre avviato un tavolo di lavoro con l'Agenzia delle dogane in merito agli aspetti di protezione dei dati personali connessi alla previsione secondo cui le associazioni che prestano attività di soccorso mediante autoambulanze, ai fini dell'emissione del buono d'imposta, debbano produrre all'Agenzia i fogli di viaggio nei quali sono registrati, fra l'altro, anche le generalità del paziente trasportato (d.m. 31 dicembre 1993). Al riguardo, l'Ufficio ha evidenziato la necessità che, ai fini dell'emissione del suddetto buono d'imposta, sia prevista l'esibizione di documenti privi di dati identificativi diretti dei soggetti trasportati dai mezzi di soccorso (note 21 gennaio e 20 novembre 2014).

Customer satisfaction in ambito sanitario

Numerose le segnalazioni relative ai trattamenti effettuati in ambito sanitario per finalità amministrative correlate alla cura: in merito ad un sondaggio effettuato da un Istituto di ricerca e cura a carattere scientifico (Irccs) sul gradimento del servizio di prenotazione *online*, richiamando le "Linee guida in tema di trattamento di dati per lo svolgimento di indagini di *customer satisfaction* in ambito sanitario" (provv. 5

maggio 2011, n. 182, doc. web n. 1812910), l'Ufficio ha sottolineato la necessità di utilizzare metodi di indagine basati sull'acquisizione di dati che consentono di identificare gli utenti anche indirettamente. In particolare, per consentire all'utente di scegliere consapevolmente se aderire o meno ad indagini di *customer satisfaction*, esprimendo le proprie valutazioni riguardo alla qualità dei servizi sanitari fruiti, gli organismi sanitari, in qualità di titolari del trattamento, sono tenuti a fornire previamente all'interessato un'idonea informativa (artt. 13, 79 e 80 del Codice). Con riferimento al caso segnalato è stato riscontrato l'utilizzo da parte dell'Istituto degli indirizzi di posta elettronica indicati dai pazienti ai fini della prenotazione *online* senza fornire loro una specifica informativa sul trattamento dei dati personali effettuato per le attività di *customer satisfaction* (con avvio del conseguente procedimento sanzionatorio: cfr. nota 22 maggio 2014).

L'Ufficio è intervenuto anche in relazione a quanto denunciato dalla stampa in merito alla circostanza che i reclami presentati dagli utenti di una azienda sanitaria locale del nord Italia, contenenti numerosi dati sanitari, fossero interamente visualizzabili sul sito internet della stessa. Modificando un parametro nell'url del *link* presentato all'utente nella pagina di conferma di inserimento della segnalazione era possibile, infatti, leggere i dati delle segnalazioni archiviate. Tali dati, non indicizzati da parte dei principali motori di ricerca, sono stati prontamente rimossi ed è stato modificato il *software* utilizzato per offrire tale servizio al fine di superare le criticità riscontrate dall'Ufficio anche con riferimento alla circostanza che lo stesso sistema era in uso presso altre aziende sanitarie del territorio (nota 14 febbraio 2014).

Rinnovo della patente e dati sanitari

A seguito di segnalazioni l'Ufficio ha interessato il Ministero delle infrastrutture e dei trasporti e quello della salute in merito al trattamento dei dati personali effettuato in occasione della redazione – a seguito dell'accertamento dei requisiti psichici e fisici – da parte della commissione medica locale del certificato medico per il rinnovo della patente di guida (art. 119, d.lgs. n. 285/1992 e artt. 320 e 331, d.P.R. n. 495/1992). L'attenzione dell'Ufficio si è concentrata sul periodo in cui l'interessato, ottenuto il rinnovo della patente, è ancora in attesa di ricevere il contrassegno di rinnovo da apporre sulla stessa da parte della Motorizzazione civile; in tale lasso di tempo, infatti, l'interessato può dover esibire alle Forze dell'ordine la suddetta certificazione contenente dati idonei a rivelare lo stato di salute. Al riguardo, l'Ufficio ha rappresentato la necessità di individuare idonee cautele volte a non far evincere in modo immediato le condizioni di salute dell'interessato in caso di esibizione della suddetta certificazione. A seguito dell'intervento dell'Ufficio, il Ministero delle infrastrutture e dei trasporti, previo parere del Ministero della salute, ha adottato un nuovo decreto in materia secondo il quale l'attestazione rilasciata all'interessato all'atto del rinnovo della patente, da esibire se richiesta alle Forze dell'ordine, sia priva di informazioni relative allo stato di salute dello stesso e contenga esclusivamente il giudizio di idoneità e le eventuali prescrizioni di legge (nota 22 maggio 2014).

Nonostante ripetute pronunce del Garante (da ultimo v. provv. 16 luglio 2013, n. 331, doc. web n. 2536504), continuano a pervenire segnalazioni in ordine al trattamento di dati sanitari contenuti nelle certificazioni che attestano il riconoscimento dell'invalidità, dell'handicap e delle condizioni di disabilità.

Verbali di accertamento dello stato di invalidità

In un caso portato a conoscenza dell'Ufficio, un'amministrazione, ai fini del riconoscimento dei benefici previsti dalla legge in favore delle persone con disabilità, pretendeva da un proprio dipendente copia integrale del verbale di accertamento dell'invalidità civile della moglie, comprensivo delle parti relative alla diagnosi. In un altro caso, una struttura sanitaria si era rifiutata di rilasciare copia del verbale di accertamento dello stato di invalidità priva dell'indicazione delle patologie riscontrate dalla commissione medica, adducendo di poter fornire solo copia integrale dello stesso.

Al riguardo, l'Ufficio ha ribadito (note 15 gennaio 2015) che per assicurare il rispetto dei principi di pertinenza, non eccedenza e indispensabilità dei dati trattati (artt. 11 e 22, commi 3 e 5, del Codice), nei procedimenti volti al riconoscimento delle agevolazioni previste dalla legge in favore dei soggetti disabili, ivi compresi i permessi e congedi in favore di lavoratori con familiari portatori di handicap, le amministrazioni possono acquisire esclusivamente documentazione dalla quale risulti la sola accertata condizione di disabilità del familiare (v. provv. 14 giugno 2007, n. 23, doc. web n. 1417809). In attuazione dei predetti principi di pertinenza, non eccedenza e indispensabilità, inoltre, le Commissioni mediche sono tenute a rilasciare copia del verbale di accertamento dello stato di invalidità, con l'omissione delle parti relative alla descrizione dei dati anamnestici, all'esame obiettivo e alla diagnosi dell'interessato (nota 15 gennaio 2015; v. già provv.ti 21 marzo 2007, doc. web n. 1395821; 16 febbraio 2011, n. 69, doc. web n. 1792975).

Comunicazione al datore di lavoro dei dati di familiare disabile da parte dell'Inps

Infine, l'Ufficio si è pronunciato sulla legittimità della comunicazione da parte dell'Inps al datore di lavoro dei soli dati identificativi del familiare disabile per il quale il lavoratore presenta domanda di congedo straordinario per gravi motivi ai sensi del d.lgs. n. 151/2001 (nota 21 gennaio 2015). In proposito, è stato rilevato che tali informazioni appaiono indispensabili, tenuto conto dei compiti che spettano al datore di lavoro in ordine alla verifica in concreto della sussistenza dei requisiti previsti dalla legge per usufruire di tali benefici. Ciò ferme restando le attribuzioni dell'Inps in merito alla verifica preventiva, sotto il profilo previdenziale, della congruità delle istanze di congedo rispetto a quanto previsto dalla legge (art. 42, comma 5 ss., d.lgs. 26 marzo 2001, n. 151; art. 4, comma 2 ss., l. 8 marzo 2000, n. 53; d.m. 21 luglio 2000, n. 278). Sul tema si è espressa di recente la giurisprudenza di legittimità (Cass., Sez. lav., 12 febbraio 2015, n. 2803).

7 I dati genetici

Come riferito (cfr. Relazione 2013, p. 75), sentito il Ministro della salute – che ha acquisito a tal fine il parere del Consiglio superiore di sanità – il Garante ha autorizzato ai sensi dell'art. 90 del Codice il trattamento dei dati genetici nell'ambito di una ricerca scientifica condotta, in assenza del consenso di tutti i pazienti coinvolti (affetti da cirrosi epatica e sottoposti a trapianto di fegato negli anni 2005-2010), con dati genetici e campioni biologici di circa duecento individui (parte dei quali deceduti) nell'ambito di uno studio svolto presso un'azienda ospedaliero-universitaria finalizzato a monitorare gli esiti clinici del trapianto (provv. 30 gennaio 2014, n. 51, doc. web n. 2939000).

Grazie ad alcune notizie stampa, l'Autorità ha appreso del fallimento e della successiva liquidazione di una società di ricerca nel campo delle biotecnologie che gestisce una banca dati contenente decine di migliaia di campioni biologici nonché dati genetici e sanitari della popolazione sarda. In merito a tale vicenda, l'Ufficio ha avviato accertamenti con particolare riferimento alla destinazione e all'eventuale cessione a terzi della banca dati. La disciplina sulla protezione dei dati personali pone specifici limiti nei casi di cessazione del trattamento, ivi compresa l'eventuale cessione dei dati (artt. 16 e 162, comma 1, del Codice), volti ad assicurare l'osservanza del principio di finalità (art. 11), in conformità alla volontà manifestata da coloro che hanno acconsentito al conferimento dei loro dati e campioni alla banca dati, nonché dell'obbligo di rendere l'informativa agli interessati anche al fine di garantire l'esercizio da parte di questi ultimi dei diritti d'accesso e degli altri diritti previsti dal Codice (artt. 7 e 13).

A fine 2014, inoltre, il Garante ha rinnovato, per la durata di due anni, l'autorizzazione generale sui dati genetici, in termini sostanzialmente analoghi alla precedente (provv. 11 dicembre 2014, n. 590, doc. web n. 3632835).

8 La ricerca scientifica e la statistica

8.1. *La ricerca scientifica*

L'autorizzazione generale n. 9 al trattamento di dati sensibili per finalità di ricerca scientifica – rinnovata fino a dicembre 2016 in termini sostanzialmente analoghi alla precedente (provv. 11 dicembre 2014, n. 591, doc. web n. 3632879) e sulla quale l'Ufficio ha fornito indicazioni generali allo scopo di promuovere una corretta attuazione delle disposizioni in materia di protezione dei dati personali – consente di trattare dati personali sulla salute (e, laddove siano indispensabili per il raggiungimento delle finalità della ricerca, dati sulla vita sessuale e sull'origine razziale ed etnica), in assenza del consenso dei pazienti interessati, per studi e ricerche in campo medico, biomedico e epidemiologico nel caso in cui risulti impossibile rendere l'informativa agli interessati, a causa, tra gli altri, di "motivi di impossibilità organizzativa". Ciò 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).

In proposito, è stato precisato che, nelle ipotesi di "impossibilità organizzativa", è possibile utilizzare i dati personali dei soli pazienti i quali, all'esito di ogni ragionevole sforzo compiuto presso i centri di cura per contattarli (ad es., attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti o l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente), risultino essere deceduti o non contattabili al momento dell'arruolamento nello studio (nota 6 maggio 2014).

L'Autorità ha altresì affrontato il tema dei trattamenti di dati personali, anche sensibili, effettuati per la realizzazione e la tenuta di registri di patologia. Al riguardo, una Asl ha chiesto all'Autorità un'autorizzazione al trattamento dei dati sensibili per la gestione di un registro tumori provinciale. Nel fornire riscontro, l'Ufficio ha avuto occasione di chiarire che, alla luce della regolamentazione dettata dalla legge regionale (che prevede la realizzazione di un registro della popolazione regionale articolato su base provinciale e sub-provinciale), le finalità del trattamento sono riconducibili al perseguimento di scopi di ricerca scientifica finalizzata alla tutela della salute in campo medico, biomedico ed epidemiologico (artt. 107 e 110 del Codice), nonché di valutazione dell'appropriatezza e dell'efficacia dell'assistenza sanitaria erogata (art. 85 del Codice). Tali attività, previste dalla legge regionale tra quelle istituzionalmente perseguite dal registro, sono inoltre qualificate dal Codice di rilevante interesse pubblico (artt. 20, 85 e 98 del Codice).

Pertanto, ai fini della legittimità del trattamento è necessario individuare, con regolamento regionale, in conformità al parere espresso dal Garante, i tipi di dati sensibili e di operazioni indispensabili per l'espletamento delle predette attività, ivi compresi i soggetti che possono avervi accesso e i dati che possono conoscere, nonché le misure per la custodia e la sicurezza dei dati. Ciò in conformità alla disciplina del Codice sul trattamento dei dati sensibili e alle disposizioni legislative nazionali intervenute nel frattempo in materia di sistemi di sorveglianza e di registri di patologia (artt. 20 e 154 del Codice; art. 12, commi 10 ss., d.l. 18 ottobre 2012, n. 179 convertito con l. 17 dicembre 2012, n. 221). In questo quadro, l'Ufficio ha messo altresì in evidenza alcuni aspetti di criticità riscontrati nella disciplina regionale di

riferimento riguardo al trattamento dei dati personali degli ammalati di tumore da parte dei diversi soggetti coinvolti nel suo funzionamento (nota 1° dicembre 2014; v. sul punto anche parere 13 settembre 2012, n. 241, doc. web n. 1927415).

Sempre con riferimento al tema dei registri di patologia, l'Ufficio ha avviato un'attività di collaborazione con talune regioni che sono in procinto di disciplinare con proprio atto regolamentare i trattamenti di dati sensibili e, in particolare, di quelli attinenti alla salute, connessi alla tenuta e al funzionamento di registri tumori su base regionale (nota 14 gennaio 2015).

Un altro caso, esaminato dal Garante a seguito di accertamenti ispettivi avviati d'Ufficio, ha riguardato un registro gestito da un'associazione scientifica di medici nefrologi che a livello nazionale raccoglie dati sanitari riferiti a pazienti con insufficienza renale cronica per finalità di ricerca scientifica in campo medico-epidemiologico (provv. 16 gennaio 2014, n. 16, doc. web n. 2937031). Nell'ambito delle verifiche svolte, è emerso che il registro era alimentato, su base volontaria, dai responsabili dei registri regionali e provinciali di dialisi e trapianto, gestiti da enti e organismi sanitari pubblici, i quali inviavano all'associazione alcuni dati clinici disaggregati riferiti ai pazienti in trattamento dialitico presso i centri dialisi territoriali. I dati raccolti erano quindi elaborati e aggregati dall'associazione per analisi statistiche ed epidemiologiche e poi trasmessi a un'associazione europea per finalità di ricerca scientifica in ambito sovranazionale.

Dagli approfondimenti compiuti è stato riscontrato che tale trattamento avveniva in assenza di idonea informativa e del consenso degli interessati: l'associazione, infatti, riteneva che i dati raccolti fossero anonimi e che, quindi, questi non fossero soggetti alla disciplina in materia di protezione dei dati personali. Al contrario, l'Autorità ha accertato che i dati trasmessi dai registri territoriali, pur non contenendo i nominativi degli interessati, erano collegati allo stesso codice univoco con cui le informazioni erano memorizzate nel registro territoriale e riportavano numerose informazioni (ad es., data di nascita, sesso, codice della nefropatia, trattamenti dialitici effettuati, risultati degli esami clinici, patologie correlate alla malattia renale) che rendevano comunque possibile re-identificare i pazienti, sia pure mediante il collegamento con altri dati nella disponibilità di terzi.

Come è noto, le persone giuridiche private che perseguono finalità di studio e di ricerca scientifica possono utilizzare dati personali attinenti alla salute, anche raccolti presso strutture pubbliche, di regola a condizione di aver fornito una previa e idonea informativa agli interessati e aver ottenuto il loro specifico consenso (artt. 106, 107 e 110 del Codice e autorizzazione generale n. 2, punto 1.2). L'obbligo di raccogliere il consenso degli interessati non è richiesto solo in casi residuali, quando ricorrono particolari condizioni, quali la previsione dello specifico trattamento in una disposizione di legge, anche regionale, o l'essere inserito in un programma di ricerca biomedica o sanitaria, oppure quando non è possibile, a causa di particolari ragioni, informare gli interessati e il programma di ricerca è oggetto di parere favorevole del competente comitato etico ed è altresì autorizzato dal Garante.

Al riguardo, l'Autorità, nel sottolineare la rilevanza degli scopi di ricerca scientifica perseguiti dall'associazione, ha evidenziato che questi non possono prescindere dalla necessità di adottare adeguate misure a tutela della riservatezza degli interessati. È stato quindi vietato all'associazione di proseguire il trattamento dei dati sanitari dei pazienti nefropatici prima di aver provveduto ad informarli e ad acquisire il loro consenso nonché ad adottare adeguate misure di sicurezza per proteggere i dati. In alternativa, l'associazione potrà raccogliere dai centri dialisi territoriali solo dati "effettivamente anonimi" (art. 4, comma 1, lett. *n*), del Codice), non soggetti alla disciplina prevista dal Codice.

Infine, l'Autorità ha appreso da notizie di stampa che una regione ha regolato con propria delibera l'accesso alla banca dati sanitaria regionale da parte di enti esterni (pubblici e privati) affidatari dell'attività di valutazione dell'appropriatezza, dell'efficacia e dell'efficienza dell'assistenza sanitaria erogata, sulla base di una convenzione e dietro eventuale corresponsione di un contributo economico a titolo di rimborso dei costi sostenuti dall'ente regionale per la messa a disposizione del proprio patrimonio informativo.

Al riguardo, l'Ufficio ha curato specifici approfondimenti, anche nell'ambito di apposite riunioni con i responsabili dell'amministrazione, all'esito dei quali la regione ha comunicato all'Autorità di voler modificare e integrare il testo della propria delibera al fine di accogliere le indicazioni suggerite volte a rendere il testo conforme alla disciplina in materia di protezione dei dati personali. A tal fine, la regione si è impegnata a sottoporre all'Autorità il testo della nuova delibera e di ogni altro atto volto ad incidere sulla definizione della materia (nota 12 novembre 2014).

8.2. *La statistica*

Il d.l. 31 agosto 2013, n. 101, convertito con modificazioni in l. 30 ottobre 2013, n. 125, ha disposto l'abrogazione dell'art. 6-*bis*, comma 2, d.lgs. n. 322/1989, a tenore del quale "nel Programma statistico nazionale sono illustrate le finalità perseguite e le garanzie previste dal presente decreto e dalla legge 31 dicembre 1996, n. 675. Il Programma indica 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. Il Programma è adottato sentito il Garante per la protezione dei dati personali" (art. 8-*bis*, comma 1, lett. *a*).

Sulla base di tale abrogata disposizione, l'Istat, prima dell'adozione dei Psn, ha acquisito annualmente il parere del Garante, apportando ai Programmi stessi, ove necessario, le opportune modifiche indicate dall'Autorità affinché nell'ambito dei trattamenti di dati personali, anche sensibili e giudiziari, effettuati per finalità statistiche ivi descritti fosse garantito il più elevato livello di tutela dei diritti, delle libertà fondamentali e della dignità degli interessati, con particolare riferimento alla loro riservatezza, identità personale e al diritto alla protezione dei dati personali (art. 2 del Codice).

Inoltre, il rispetto della procedura prevista dall'abrogato art. 6-*bis*, comma 2, d.lgs. n. 322/1989, costituiva anche idoneo presupposto di legittimità per il trattamento di dati sensibili e giudiziari effettuato nell'ambito dei lavori statistici previsti dal Psn, alternativo alle regole generali poste dal Codice per il trattamento di tali categorie di dati personali (artt. 20-22 del Codice).

Ciò premesso, l'Istat, istituzionalmente tenuto a provvedere all'esecuzione delle rilevazioni statistiche previste nel Psn (art. 15, comma 1, lett. *b*), d.lgs. n. 322/1989), in un'ottica di semplificazione e anche al fine di garantire il rispetto delle specifiche garanzie previste per il trattamento dei dati sensibili e giudiziari, acquisiti i pareri del Ministero per la semplificazione e la pubblica amministrazione, del Comstat e della Commissione per la garanzia della qualità dell'informazione statistica (art. 12, d.lgs. n. 322/1989 e art. 3, d.P.R. n. 166/2010), ha avanzato al Garante la proposta di inserire nel codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, All. A.3. al Codice, adottato con provv. 31 luglio 2002, n. 13 (doc. web n. 1556573) un nuovo articolo 4-*bis*, in base al quale "nel Programma statistico nazionale sono illustrate le finalità perseguite e le garanzie previste dal d.lgs. 6 set-

tembre 1989, n. 322 e dal d.lgs. 30 giugno 2003, n. 196 e dal presente codice deontologico. Il Programma indica altresì i dati di cui all'art. 4, comma 1, lett. *d*) ed *e*), d.lgs. 30 giugno 2003, n. 196, le rilevazioni per le quali i dati sono trattati e le modalità di trattamento. Il Programma è adottato, con riferimento ai dati personali, sensibili e giudiziari, sentito il Garante per la protezione dei dati personali, ai sensi dell'art. 154 del d.lgs. 30 giugno 2003, n. 196". Ciò in quanto il citato codice di deontologia reca la disciplina del trattamento di dati personali effettuato dai soggetti che fanno parte del Sistema statistico nazionale, in particolare per quanto riguarda il trattamento dei dati sensibili e giudiziari indicati nel Psn, e considerato che il rispetto delle disposizioni contenute nel codice di deontologia è condizione essenziale per la liceità del trattamento dei dati personali (artt. 12, 106 e 108 del Codice).

Al riguardo, il Garante, considerati i ruoli del Comstat, della Commissione e dell'Istat in relazione all'adozione del Psn, ha condiviso la proposta di modifica del codice di deontologia presentata, nel rispetto del principio di rappresentatività, dai soggetti maggiormente interessati nella predisposizione del Psn (art.12 del Codice; artt. 12, comma 1, lett. *c*), 13, comma 3, e 15, comma 1, lett. *a*) e *b*), d.lgs. n. 322/1989; art. 5, comma 1, d.P.C.M. 28 aprile 2011; art. 3, comma 6, d.P.R. n. 166/2010). Nel merito, l'Autorità ha poi ritenuto che detta modifica consenta al Garante di poter effettuare le valutazioni di competenza relative al rispetto della disciplina in materia di protezione dei dati personali, con particolare riferimento alle garanzie previste per il trattamento dei dati sensibili e giudiziari (art. 22 del Codice). Su tali basi, ai sensi dell'art. 12, comma 2, del Codice, l'Autorità ha disposto l'integrazione del codice di deontologia con il sopra richiamato articolo 4-*bis*, rubricato "Trattamento di dati personali, sensibili e giudiziari, nell'ambito del Programma statistico nazionale" (provv. 12 giugno 2014, n. 296, doc. web n. 3268032).

Alla luce delle riforme normative sopra evidenziate, il Garante ha reso il parere di competenza sullo schema di Programma statistico nazionale 2014-2016 (di seguito Psn) ai sensi dell'art. 4-*bis* del codice di deontologia.

Anche tale parere, favorevole, è stato emanato all'esito di un'intensa collaborazione con l'Istat, volta a garantire un elevato *standard* di tutela del diritto alla protezione dei dati personali nell'ambito dei trattamenti effettuatati per lo svolgimento dei lavori della statistica ufficiale (provv. 26 giugno 2014, n. 324, doc. web n. 3320710). In particolare, in tale Psn, l'Istat ha recepito le indicazioni dell'Ufficio in relazione all'informativa da rendere agli interessati ai sensi dell'art. 13 del Codice e 6, comma 2, del codice di deontologia, integrandola con i necessari chiarimenti in relazione alle singole componenti di cui essa deve essere composta (artt. 13 e 22, comma 2, del Codice). Come negli anni precedenti, il Psn prevede che l'informativa sia contenuta in un paragrafo del programma, oltre che nei singoli prospetti identificativi dei lavori statistici, fermo restando l'obbligo di fornire preventivamente idonea informativa agli interessati per le rilevazioni che prevedono la raccolta diretta di dati personali presso gli stessi.

In tale ambito, sono altresì state evidenziate le specifiche indicazioni in relazione alla "natura obbligatoria o facoltativa del conferimento dei dati". In particolare, nel ribadirsi che non sussiste obbligo di risposta per i dati sensibili e giudiziari – a meno che esso non sia previsto da un'espressa disposizione normativa –, è stato precisato che, nelle ipotesi di lavori statistici che comportano la raccolta presso soggetti terzi delle predette categorie di dati personali, è garantita, attraverso l'adozione di specifiche misure organizzative, la possibilità per l'interessato di aderire facoltativamente al trattamento statistico delle predette informazioni. Tale circostanza è stata, inoltre, opportunamente richiamata anche nei singoli prospetti identificativi, fatta eccezione per quelli inerenti ai lavori statistici che prevedono la raccolta di dati perso-

nali direttamente presso gli interessati e per quelli per i quali l'obbligo di risposta non sussiste in ogni caso: "indagini dirette collegate" effettuate nell'ambito degli Studi progettuali (identificati con la sigla Stu), Statistiche derivate o rielaborazioni (Sde) e per i Sistemi informativi statistici (Sis).

Facendo seguito alla raccomandazione resa dal Garante nel parere sul Psn 2011-2013, aggiornamento 2013 (cfr. parere 20 settembre 2012, n. 249, doc. web n. 2069239), il Psn fornisce idonei chiarimenti sul ruolo dei cd. "compartecipanti", distinguendo quanti collaborano alla realizzazione del lavoro, senza tuttavia trattare dati personali, da coloro che realmente sono coinvolti nelle operazioni di trattamento, questi ultimi, come evidenziato nel Programma, designati responsabili del trattamento ai sensi dell'art. 29 del Codice.

Sulla base delle indicazioni dell'Ufficio, l'Istat, al fine di informare adeguatamente gli interessati circa le finalità statistiche perseguite, laddove necessario ha riformulato, in termini più chiari, la descrizione dell'obiettivo statistico (art. 13, comma 1, lett. *a*), del Codice; ad es., IST-02546 *Micro demographic accounting* (MIDEA); EMR-00021 Sistema informativo della popolazione da circolarità anagrafica- sistema ANA-CNER; IPS-00020 Certificati di diagnosi per indennità di malattia; IST-02507 Analisi ai fini statistici delle Anagrafi nazionali degli studenti delle scuole e delle università; IPS-00042 Lavoratori parasubordinati; PBL-00004 SIS-Belluno: Sistema statistico sul mercato del lavoro; IPS-00009 Prestazioni dell'assicurazione contro la tubercolosi; IST-02481 Rilevazione integrativa sugli scambi con l'estero di merci e servizi).

Con riferimento all'analisi dei singoli lavori statistici si evidenzia, in primo luogo, che è stata posta particolare attenzione ad una nuova tipologia di lavoro consistente nella realizzazione di cd. *Repository*. Trattasi di basi di dati integrate (archivi amministrativi e fonti statistiche) volti alla realizzazione di archivi statistici intermedi, utili all'Istat per svolgere successive elaborazioni, anche di tipo longitudinale, nei diversi settori di interesse (ad es., IST-02520 Sviluppo di archivi statistici intermedi su unità socio-economiche – SIM; IST-02264 Base integrata di microdati statistici per l'analisi dell'occupazione; Sistema di integrazione logico-fisica di microdati amministrativi e statistici-SIM IST-02270).

Al riguardo, è stato ribadito (cfr. pareri 10 giugno e 23 settembre 2010, rispettivamente doc. web nn. 1734415 e 1753181) che i dati sensibili e giudiziari contenuti in elenchi, registri e banche dati devono essere resi momentaneamente inintelligibili anche a chi è autorizzato ad accedervi, permettendo l'identificazione degli interessati solo in caso di necessità e che i dati idonei a rilevare lo stato di salute e la vita sessuale devono essere conservati separatamente da altri dati personali che non richiedono il loro utilizzo (art. 22, commi 6 e 7, del Codice).

In secondo luogo, l'Istat, nel recepire le indicazioni dell'Ufficio, nei prospetti identificativi relativi a due lavori statistici inerenti, rispettivamente, la sindrome dell'Aids e il virus dell'HIV, considerato che tra i principali caratteri statistici rilevati vi sono anche i "fattori di rischio", ha evidenziato tra i dati sensibili trattati, anche quelli idonei a rivelare la vita sessuale, precisando, al contempo, la definizione di "fattori di rischio" (contatto eterosessuale o contatto omosessuale) (ISS-00004 Registro nazionale aids; ISS-00043 Sistema di Sorveglianza delle nuove diagnosi di infezione da HIV).

Con riferimento, infine, ai lavori statistici che prevedono la raccolta presso soggetti minori di età di dati sensibili o comunque inerenti aspetti particolarmente intimi della vita privata degli stessi idonei ad incidere sulla loro dignità (es. struttura familiare, soddisfazione vita quotidiana; condizioni di salute; tipo di esperienze sentimentali/sessuali, eventuali molestie, metodi anticoncezionali; intervalli di tempo

di lavoro retribuito; grado di soddisfazione della vita quotidiana), anche facendo seguito alle precedenti raccomandazioni del Garante (parere 20 settembre 2012, n. 249, doc. web n. 2069239), l'Istat ha previsto, nel Psn in esame, che la raccolta delle informazioni relative a minori infraquattordicenni avvenga per il tramite dei genitori o di un adulto di riferimento che risponde per il minore. Per gli infradiciottenni, invece, la rilevazione viene effettuata attraverso PC o altri strumenti informatici che escludono la presenza di un intervistatore che potrebbe suscitare sentimenti di soggezione o imbarazzo nell'interessato.

Con provvedimento del 18 settembre 2014, n. 411 (doc. web n. 3458502) il Garante ha fornito, ai sensi dell'art. 4-*bis* del codice di deontologia, il parere di competenza sul Programma statistico nazionale 2014-2016 aggiornamento 2015-2016 (Psn). In particolare, il parere è stato reso in relazione al trattamento di dati personali inseriti per la prima volta nel Psn ed alle modifiche apportate ai prospetti ai lavori statistici che comportano il trattamento di dati personali già inclusi nel Psn 2014-2016.

In tale ambito, l'Autorità ha formulato alcune osservazioni in relazione a specifici lavori statistici. In particolare, sulla base delle indicazioni dell'Ufficio, l'Istat ha convenuto di modificare la scheda informativa relativa al lavoro statistico "Prestazioni economiche di malattia e maternità"-IPS-00052, specificando che esso comporta altresì, come si evince anche dalla denominazione dello stesso, il trattamento di dati sensibili idonei a rivelare lo stato di salute degli interessati.

Nell'ambito dell'attività istruttoria è stata inoltre posta particolare attenzione al lavoro statistico "Uso a fini statistici dei *Big Data*" IST-02589. Con tale locuzione l'Istat ha voluto fare riferimento ai dati di telefonia mobile, elaborati a fini di programmazione e gestione dei servizi locali e individuazione di opportune misure di protezione civile. In particolare, le informazioni di telefonia mobile trattate riguardano un sottoinsieme delle variabili registrate del gestore telefonico durante una chiamata, denominato *call detail record* (cdr). Il cdr è un "progressivo" (sostitutivo del codice fiscale, nome e cognome, corrispondente all'utente) al quale, per la rilevazione statistica, vanno aggiunte le informazioni relative al comune nel quale si trova la cella di effettuazione della chiamata, la data e ora della stessa.

Al riguardo, l'Istat su specifica richiesta dell'Ufficio, ha fornito idonee assicurazioni sulla natura anonima dei dati raccolti presso il gestore telefonico. A tal fine quest'ultimo assegna un codice ad ogni cdr eliminando successivamente ogni possibilità di raccordo tra tale codice e gli identificativi originali.

I *big data* rappresentano un ampio patrimonio informativo e l'utilizzo di queste informazioni comporta specifici rischi per l'effettiva tutela della riservatezza degli interessati e la corretta applicazione della disciplina in materia di protezione personali, tenuto anche conto che grazie alle nuove tecnologie e alle nuove tecniche di analisi, mediante l'elaborazione e l'interconnessione dei dati risulta possibile re-identificare un interessato anche attraverso informazioni apparentemente anonime (cd. *single-out*).

Su tali basi, è stata posta particolare attenzione anche all'analisi delle successive modalità di trattamento dei dati anonimi raccolti dall'Istat presso il gestore telefonico.

Al riguardo, l'Istituto ha precisato che la sperimentazione è volta a stimare i flussi intercomunali a livello aggregato e non individuale. In ordine, poi, all'eventuale rischio di re-identificazione derivante dalla possibilità di individuare un'unità elementare tramite collegamento – indiretto – ad altre fonti di dati in possesso dell'Istituto, su specifica richiesta dell'Ufficio è stata fornita idonea assicurazione che, nell'ipotesi in cui dovessero verificarsi frequenze di flusso inferiori a tre unità, le stesse verranno oscurate.

L'Istat ha infine precisato che i dati e le procedure descritte verranno utilizzate, con riferimento ai dati di telefonia mobile della sola provincia di Pisa nel mese di ottobre 2011, a fini esplorativi, di sperimentazione e messa a punto di applicativi per la stima di flussi aggregati che verranno in futuro gestiti direttamente dai gestori telefonici. L'Autorità si è riservata di effettuare verifiche anche in relazione ai trattamenti effettuati dai gestori telefonici.

Nell'ambito dei lavori volti a diffondere le stime di povertà ed esclusione sociale sono emerse alcune criticità in relazione al lavoro statistico "Povertà e deprivazione trasversale e longitudinale" - IST-01961 teso, appunto, alla rilevazione delle predette informazioni. In particolare l'Istat ha rappresentato l'intenzione di integrare tale lavoro, così come presente nel Psn 2014-2016, con il trattamento di dati personali, anche sensibili (origine razziale ed etnica, stato di salute) provenienti da trattamenti statistici di titolarità di soggetti rientranti nel Sistema statistico nazionale-Sistan (cd. soggetti Sistan) non presenti nel Psn (enti pubblici) nonché di enti "non Sistan" (associazioni).

Sul punto è stata rilevata la carenza, nella scheda identificativa del lavoro, di informazioni sufficienti all'Autorità per formulare il proprio parere. Infatti, lo stato ancora embrionale del progetto non consentiva all'Istat di evidenziare gli enti pubblici ovvero le associazioni presso i quali raccogliere i dati; il formato anonimo, aggregato (e in tal caso con che livello di aggregazione) ovvero individuale degli stessi e, nel caso di raccolta di dati personali non aggregati, le modalità previste per garantire la volontarietà dell'adesione alla ricerca da parte degli interessati. A causa delle genericità di tali elementi informativi, inoltre, la scheda informativa del lavoro statistico non risultava tale da costituire idonea informativa ai sensi dell'art. 13 del Codice e dell'art. 6, comma 2, del codice di deontologia. Su tali basi, per il trattamento di dati personali, anche sensibili, provenienti da trattamenti statistici, di titolarità di soggetti Sistan, non presenti nel Psn, nonché di enti non Sistan, l'Istat deve sottoporre al Garante, per l'acquisizione del parere di competenza, la relativa scheda identificativa IST-01961, opportunamente integrata e fornire preventivamente idonea informativa agli interessati (13 del Codice e dell'art. 6, comma 2, del codice di deontologia).

Il Garante ha così reso parere favorevole sul Programma statistico nazionale 2014-2016 Aggiornamento 2015-2016 con le indicazioni sopra riportate relative al lavoro statistico IST-01961 (provv. 18 settembre 2014, n. 411, doc. web n. 3458502).

Social card

Parere favorevole è stato espresso sui questionari da somministrare ai soggetti coinvolti nella sperimentazione della nuova *social card*, prevista dal d.l. 9 febbraio 2012, n. 5 (provv. 10 luglio 2014, n. 356, doc. web n. 3320745).

In particolare, l'art. 60, d.l. 9 febbraio 2012, n. 5, convertito con modificazioni in l. 4 aprile 2012, n. 35, recante "Disposizioni urgenti in materia di semplificazione e di sviluppo" prevede, nei comuni con più di 250.000 abitanti, l'avvio di una sperimentazione "al fine di favorire la diffusione della carta acquisti, istituita dall'articolo 81, comma 32, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, tra le fasce di popolazione in condizione di maggiore bisogno, anche al fine di valutarne la possibile generalizzazione come strumento di contrasto alla povertà assoluta", affidandone l'attuazione ad un decreto del Ministero del lavoro e delle politiche sociali (di seguito, Ministero) adottato di concerto con il Ministero dell'economia e delle finanze (Mef).

Su tale base normativa, il Ministero ha pertanto adottato il decreto del 10 gennaio 2013, recante disposizioni per l'attuazione della sperimentazione della nuova carta acquisti, che prevede in più fasi il coinvolgimento del Garante.

Tale decreto dispone, in particolare, che i Comuni destinatari della sperimentazione individuino due gruppi nell'ambito dei nuclei familiari beneficiari della *social*

card. Uno di tali gruppi è destinato a partecipare: i nuclei familiari appartenenti al primo gruppo partecipano ad un progetto personalizzato volto al superamento della condizione di povertà, al reinserimento lavorativo e all'inclusione sociale; i nuclei familiari appartenenti al secondo gruppo, invece, pur ricevendo la *social card*, non sono coinvolti nel predetto progetto personalizzato e costituiscono un gruppo di controllo. A tale ultimo gruppo è affiancato un ulteriore gruppo di controllo composto da non beneficiari della *social card* (artt. 1, comma 1, lett. *b*), *d*) e *g*) e 3, comma 1, lett. *c*) ed *f*) del decreto).

La sperimentazione della *social card* è oggetto di valutazione da parte del Ministero, di concerto con il Mef, da realizzarsi secondo quanto descritto in un apposito progetto di ricerca, redatto in conformità all'art. 3 del codice di deontologia e buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, All. A.4. al Codice (di seguito codice di deontologia). Tale valutazione intende principalmente accertare l'efficacia dell'integrazione del sussidio economico con i servizi a sostegno dell'inclusione attiva nel favorire il superamento della condizione di bisogno (art. 9 del decreto).

Per la realizzazione del progetto di ricerca in questione, i Comuni, designati responsabili del trattamento dal Ministero e dal Dipartimento del tesoro del Mef, collaborano somministrando questionari, predisposti dal Ministero "con l'assenso del Garante per la protezione dei dati personali", ai nuclei familiari beneficiari e al gruppo di controllo dei non beneficiari all'avvio e al termine della sperimentazione (art. 9 del decreto).

In tale quadro il Ministero ha quindi chiesto il previsto "assenso" del Garante sui questionari che intende somministrare "agli adulti ed ai bambini suddivisi in fasce di età 8-13 anni e 14-17 anni".

L'Autorità ha reso il parere di competenza su una versione dei questionari, predisposti nell'ambito del piano di valutazione elaborato dal Ministero di concerto con il Mef e con la collaborazione dell'Isfol, che tiene conto delle indicazioni e degli accorgimenti forniti dall'Ufficio ai competenti uffici del Ministero nel corso di numerosi incontri, anche informali, volti a garantire che le predette rilevazioni avvengano nel rispetto della disciplina in materia di protezione dei dati personali, con specifico riferimento alla tutela dei diritti fondamentali e alla dignità degli interessati coinvolti.

In tale ambito, il Ministero ha provveduto, in particolare, a collocare l'informativa (art. 13 del Codice e art. 6 del codice di deontologia) in posizione tale che gli interessati possano prenderne visione prima della sottoposizione alle domande che compongono i questionari. Il Ministero ha inoltre accolto il suggerimento dell'Ufficio di privilegiare, nella redazione dell'informativa, un registro piuttosto colloquiale, tale da risultare agevolmente comprensibile agli interessati. Inoltre, con specifico riferimento ai questionari, accanto ad ogni quesito dal quale è possibile desumere informazioni sensibili, è stato correttamente evidenziato che, in tali ipotesi, non sussiste obbligo di risposta, con ciò ribadendo quando già precisato nell'informativa (art. 9, comma 6, lett. *a*), del decreto).

In particolare, il Garante ha verificato che le informazioni raccolte con i questionari fossero pertinenti, non eccedenti e, con riferimento ai dati sensibili e giudiziari, indispensabili rispetto alle finalità che con essi si intende perseguire (artt. 11 e 22 del Codice e art. 9 del decreto).

9 I trattamenti da parte di Forze di polizia

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

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

9.2. *Altri interventi in relazione alle Forze di polizia*

Microtelecamere mobili alle manifestazioni

Il Dipartimento della pubblica sicurezza del Ministero dell'interno ha chiesto al Garante di valutare un progetto sperimentale di ripresa visiva nel corso dello svolgimento di pubbliche manifestazioni, attraverso l'assegnazione a personale specificamente individuato di Reparti Mobili della Polizia di Stato di microtelecamere per l'eventuale ripresa di quanto avviene in situazioni di criticità per l'ordine pubblico.

Esaminato il progetto, il Garante ha rilevato che il trattamento di dati personali così effettuato appare finalizzato alla tutela dell'ordine e della sicurezza pubblica, la prevenzione, l'accertamento o la repressione dei reati e, quindi, sulla base delle disposizioni vigenti in materia di ordine pubblico, rientra nelle previsioni di cui all'articolo 53 del Codice, che esclude l'applicabilità a tali fattispecie di alcune disposizioni del Codice stesso (nota 31 luglio 2014, doc. web n. 3423775).

Il Garante, tuttavia, ha ricordato che anche i trattamenti di cui all'art. 53 del Codice debbono rispettare i principi di cui all'art. 11 del Codice medesimo, sicché i dati personali oggetto di trattamento debbono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, nonché conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

È stato pertanto indicato che il sistema di ripresa video sopra descritto dovrà essere attivato solo in caso di effettiva necessità, ossia di insorgenza di concrete e reali situazioni di pericolo di turbamento dell'ordine e della sicurezza pubblica. È pertanto opportuno che l'attività di formazione del personale di polizia destinato ad utilizzare i sistemi di ripresa – e, segnatamente, dei funzionari deputati a disporne l'attivazione e lo spegnimento – riguardi anche le regole concernenti la protezione dei dati personali; inoltre, in caso di effettuazione di riprese in occasione di situazioni di ritenuto pericolo per l'ordine e la sicurezza pubblica poi non concretizzatosi, venga disposta la tempestiva cancellazione delle immagini riprese in quanto il loro ulteriore trattamento risulterebbe estraneo alle finalità di cui all'art. 53 del Codice. Analogamente, è necessario che le immagini siano conservate per il solo tempo necessario al perseguimento delle finalità sottese al trattamento e che, al termine, esse siano cancellate. Dovranno inoltre essere designati gli incaricati del trattamento e adottate le misure di sicurezza di cui agli artt. 31 e ss. del Codice.

E.T.Na.

È stato espresso dal Garante parere favorevole (provv. 15 maggio 2014, n. 244, doc. web n. 3259425) sullo schema di Convenzione tra il Ministero dell'interno e i gestori di servizi di telecomunicazioni che regola l'accesso telematico delle Forze di polizia – previsto dalla legge e autorizzato solo per finalità di giustizia – a taluni dati riferiti ai detentori di telefoni fissi e mobili, tramite il Centro di elaborazione dati (Ced) del Dipartimento della pubblica sicurezza, utilizzando uno specifico sistema informatico denominato Elenco Telefonico Nazionale (E.T.Na.).

Gli approfondimenti al riguardo intercorsi su alcuni aspetti della Convenzione hanno consentito di introdurre maggiori garanzie per i possessori di telefoni fissi e mobili.

Il sistema consente la consultazione delle banche dati dei vari gestori e non comporta la creazione di un nuovo archivio né la duplicazione di informazioni. Tutti gli accessi ai dati saranno tracciati e potranno avvenire solo da postazioni di lavoro certificate; il personale che consulta il sistema dovrà essere in possesso di specifici profili di abilitazione e credenziali di autenticazione personali.

Il flusso di comunicazione dovrà essere protetto da elevati *standard* di sicurezza e non potranno essere utilizzati dispositivi automatici che consentono di consultare i dati in forma massiva.

Per i gestori tlc è stato tra l'altro introdotto l'obbligo di trasmettere al Ced un *report* delle attività di monitoraggio e controllo delle operazioni effettuate dal personale che utilizza E.T.Na.

Banca dati nazionale del dna

Come anticipato (cfr. par. 3.4), il Garante ha espresso il proprio parere su uno schema di regolamento recante disposizioni di attuazione della legge 30 giugno 2009, n. 85 (di "ratifica" del "Trattato di Prüm" relativo alla cooperazione transfrontaliera per contrastare, in particolare, il terrorismo, la criminalità transfrontaliera e la migrazione illegale) per il funzionamento della Banca dati nazionale del dna e del relativo Laboratorio centrale, istituiti, rispettivamente, presso il Ministero dell'interno-Dipartimento della pubblica sicurezza e presso il Ministero della giustizia-Dipartimento dell'amministrazione penitenziaria.

La Banca dati è istituita "al fine di facilitare l'identificazione degli autori dei delitti" (art. 5, comma 1, l. n. 85/2009) e, a tal fine, provvede alla raccolta dei profili del dna di soggetti tassativamente indicati (sottoposti a custodia cautelare, a detenzione o a misura di sicurezza detentiva, per delitti, non colposi, per i quali sia consentito l'arresto facoltativo in flagranza, con esclusione di alcune fattispecie di reato), relativi a reperti biologici acquisiti nel corso di procedimenti penali, di persone scomparse o loro consanguinei, di cadaveri e resti cadaverici non identificati, consentendone il raffronto a fini di identificazione. Il Laboratorio centrale provvede, a sua volta, alla tipizzazione del profilo del dna dei soggetti e alla conservazione dei campioni biologici dai quali sono tipizzati i profili del dna. Il controllo sulla Banca dati è esercitato dal Garante nei modi previsti dalla legge.

Con il medesimo provvedimento l'Autorità ha espresso anche la prevista "intesa" con le amministrazioni interessate sui tempi per i quali i profili del dna restano inseriti nella Banca dati, che non possono essere superiori a 40 anni dall'ultima circostanza che ne ha determinato l'inserimento, e quelli di conservazione dei campioni biologici, che non possono superare i 20 anni (artt. 13, comma 4, e 16, l. n. 85/2009).

Lo schema di regolamento disciplina le modalità di trattamento e di accesso per via informatica e telematica ai dati raccolti nella Banca dati e nel Laboratorio, le modalità di comunicazione dei dati e delle informazioni richieste, le tecniche e le modalità di analisi e conservazione dei campioni biologici, nonché i tempi di conservazione dei campioni biologici e dei profili del dna nonché le modalità di cancellazione dei profili del dna e di distruzione dei relativi campioni biologici nei casi previsti.

Anche in considerazione dell'importanza della materia e della delicatezza dei trattamenti lo schema di regolamento è stato attentamente elaborato nell'ambito di un tavolo di lavoro istituito presso il Ministero dell'interno, cui ha partecipato, fin dalla sua costituzione, anche l'Ufficio.

Nel corso delle numerose riunioni, delle interlocuzioni e degli approfondimenti anche informali che ne sono seguiti, l'Autorità ha formulato rilievi e fornito indicazioni volte a rendere il testo conforme alla disciplina in materia di protezione dei dati personali. Le indicazioni hanno riguardato, in particolare, l'esigenza di individuare tempi di conservazione dei profili del dna e dei campioni biologici proporzionati rispetto alle finalità perseguite in linea con i criteri individuati dalla normativa europea (gravità del reato commesso, pericolosità del soggetto); di individuare altresì le operazioni di trattamento dei dati consentite al personale, specificamente abilitato e incaricato del trattamento dei dati personali, in servizio presso i laboratori delle Forze di polizia, il Laboratorio centrale e la stessa Banca dati, rispetto alle finalità in concreto perseguite e le relative modalità del trattamento; di definire le responsabilità sotto il profilo della protezione dei dati dei soggetti coinvolti, a vario titolo, nell'applicazione del regolamento, ovvero in relazione ai trattamenti di dati personali effettuati, rispettivamente, dai titolari, dai responsabili e dagli incaricati del trattamento; di pervenire ad una più chiara descrizione della configurazione della Banca dati sui previsti due livelli, sia rispetto ai dati raccolti in essi, sia in relazione alle finalità rispettivamente perseguibili mediante il loro trattamento, al fine di assicurarne la compatibilità, anche sotto il profilo tecnico, con il quadro normativo vigente, nazionale ed europeo; di addivenire ad un'adeguata regolamentazione degli aspetti di sicurezza dei sistemi e del trattamento dei dati personali, volta ad assicurare elevati *standard* di protezione, fisica e logica, delle informazioni raccolte nella banca dati e dei dati trattati per il funzionamento dei laboratori; di dettare una puntuale disciplina transitoria che regoli la confluenza nella banca dati dei profili del dna acquisiti nel corso di procedimenti penali anteriormente alla data di entrata in vigore della legge n. 85/2009, nei limiti di quanto consentito dal dettato normativo; di definire una puntuale disciplina degli scambi informativi con gli altri Paesi UE per finalità di cooperazione transfrontaliera in conformità a quanto disposto dalla normativa europea (Decisioni del Consiglio UE nn. 615 e 616 del 2008).

Banca nazionale unica della documentazione antimafia

Parere favorevole è stato altresì espresso su uno schema di regolamento – proposto dal Ministro dell'Interno – volto a definire le modalità di funzionamento e collegamento della Banca nazionale unica della documentazione antimafia con il Ced interforze del Dipartimento della pubblica sicurezza ed altre banche dati, emanato in attuazione dell'art. 99, comma 1, d.lgs. 6 settembre 2011, n. 159 (cd. "codice antimafia"). L'archivio consentirà di semplificare il rilascio della documentazione antimafia sulle imprese (cd. "comunicazioni" e "informazioni" antimafia) alle stazioni appaltanti e agli altri soggetti legittimati ad acquisirle (pubbliche amministrazioni, camere di commercio, ordini professionali, ecc.). I dati registrati potranno essere trattati elettronicamente solo attraverso terminali attivati presso le Prefetture e presso gli altri soggetti legittimati all'accesso. Considerata la delicatezza e la mole dei dati, per interrogare l'archivio occorrerà utilizzare credenziali di autenticazione in base a specifici profili di autorizzazione. Tutti i dati saranno sottoposti a cifratura e verrà conservata la registrazione degli accessi. Le informazioni potranno essere trattate anche per finalità di applicazione delle normative antimafia oltre che dalle Prefetture anche da alcuni uffici del Dipartimento della pubblica sicurezza del Ministero dell'interno, dalle Forze di polizia, dalla struttura tecnica del Comitato di coordinamento per l'alta sorveglianza delle grandi opere e, nell'ambito delle attività di coordinamento del procuratore nazionale antimafia, dalla Direzione nazionale antimafia. Il parere dell'Autorità

è stato reso su una versione dello schema già perfezionata in coerenza con le indicazioni suggerite dall'Ufficio, che hanno riguardato, in particolare, le finalità del trattamento dei dati, la specificazione delle banche dati collegate, una maggiore selettività degli accessi, l'obbligo di cancellazione dei dati alla scadenza dei termini di conservazione, la previsione espressa del conforme parere del Garante sulle convenzioni che dovranno disciplinare i collegamenti con alcuni sistemi informativi e l'aggiornamento da parte dell'impresa delle informazioni ad essa riferite presenti nella banca dati.

Droni

Sono stati chiesti chiarimenti da parte del Ministero dell'interno sull'utilizzo di droni, prospettandone l'ascrivibilità alla generale categoria della videosorveglianza (art. 2.2. lett. *a*), classe B, d.m. n. 269/2010), anche in relazione alle eventuali prescrizioni da emanare, con riferimento al regolamento di servizio necessario per l'utilizzo della tecnologia in parola.

Al riguardo, si è rilevato trattarsi di materia con implicazioni estese – poiché gli apparecchi possono essere usati per scopi assai diversi – e delicate, per i rischi specifici che possono derivarne per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati acquisibili ed alle modalità del trattamento.

In questo quadro, nel rappresentare che il tema è oggetto di analisi da parte dell'Autorità nell'ambito del Gruppo Art. 29 (cfr. par. 23.3), ci si è limitati per il momento a rappresentare che non sembrano automaticamente riferibili ai droni le determinazioni del Garante in materia di videosorveglianza.

In tal senso l'art. 22 del regolamento Enac sui mezzi aerei a pilotaggio remoto del 16 dicembre 2013, entrato in vigore il 30 aprile 2014, sottopone il trattamento di dati personali effettuato tramite gli strumenti in parola al rispetto del Codice, con particolare riguardo all'utilizzo di modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3 del Codice) nonché delle misure e degli accorgimenti a garanzia dell'interessato prescritti dal Garante.

Più dettagliate valutazioni in ordine ad ipotesi di utilizzo degli apparecchi potranno quindi essere formulate – alla luce delle valutazioni risultanti in ambito europeo – sia in esito ad una verifica preliminare, ai sensi dell'art. 17 del Codice, richiesta dagli operatori che vi abbiano interesse, sia nel fornire parere, ai sensi dell'art. 154, comma 4, del Codice, in ordine a schemi di atti di carattere generale volti a disciplinare la materia.

È pervenuto un quesito relativo alle modalità di raccolta dei dati personali da parte della Guardia di finanza nel corso dello svolgimento di una verifica fiscale presso uno studio legale. Al riguardo, si è rappresentato che, in termini generali, questa Autorità non ha tra i suoi compiti istituzionali la risposta a quesiti e, di regola, non fornisce riscontro ove essi siano posti da soggetti professionalmente chiamati ad interpretare le norme di legge e ad esprimersi sulla loro applicazione. Pertanto, salvo ogni apprezzamento dell'interessato in relazione al caso concreto, si è osservato che a dati trattati con l'ausilio di strumenti elettronici da organi uffici o comandi di polizia è applicabile l'art. 56 del Codice, che rinvia alle procedure disciplinate dall'art. 10, l. n. 121/1981.

9.3. *Il controllo sul sistema di informazione Schengen*

Accertamenti disposti dal Garante

Il Ministero dell'interno-Dipartimento della pubblica sicurezza ha rappresentato l'opportunità di differire l'adempimento delle misure non ancora attuate tra quelle prescritte dal Garante volte a rafforzare la sicurezza nel trattamento dei dati effettuati per l'attuazione della Convenzione di Schengen, in ragione sia delle innova-

zioni 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 il provv. 31 luglio 2014, n. 391 (doc. web n. 3471761), ha disposto il differimento dei termini per l'adempimento delle prescrizioni, che sono in corso di attuazione.

Accesso diretto

Come è noto, 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 hanno anche quest'anno subito un lieve calo rispetto all'anno precedente.

Sono invece rimaste sostanzialmente stabili 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.

10 L'attività giornalistica

Costante è stato l'impegno rivolto alla valutazione di segnalazioni e reclami concernenti casi di trattamenti di dati personali effettuati nell'esercizio dell'attività giornalistica. Come in passato, ciò è avvenuto, tenendo anche conto delle diverse modalità con cui si esercita l'attività di informazione, avendo come principale quadro di riferimento normativo il Codice (in particolare, gli artt. 136-139) e l'allegato codice di deontologia, in un'ottica di bilanciamento tra libertà di informazione e diritto alla riservatezza e alla protezione dei dati personali. In più casi, questo problema si è posto con riferimento ai dati personali di personaggi pubblici (uomini politici e appartenenti al mondo dello spettacolo), specie quando i loro dati sono stati acquisiti mediante artifici e raggiri (cfr. par. 10.3).

Un nuovo filone di provvedimenti del Garante è quello dei ricorsi che i cittadini hanno presentato contro Google nei casi di mancato accoglimento da parte della società di richieste di deindicizzazione di dati personali presentate in attuazione dei principi affermati in una recente sentenza della Corte di giustizia dell'Unione europea (cfr. par. 10.4) tenendo altresì contro dei criteri dettati dal Gruppo Art. 29 (v. WP 225, doc. web n. 3876849).

10.1. *I minori*

Prostituzione minorile

Con riferimento al rapporto tra libertà di informazione e tutela della riservatezza dei minori, il Garante è intervenuto nei confronti di alcune testate giornalistiche che, nel dar conto di vicende concernenti alcune studentesse minorenni hanno riportato dettagli eccedenti (idonei ad identificare le interessate) tratti da brani di intercettazioni e dalle dichiarazioni delle ragazze. Il Garante, da un lato, ha vietato alle testate di riportare i dati personali riferiti alle minorenni; dall'altro, ha richiamato i media e i gestori di siti web al più rigoroso rispetto dei principi a tutela dei minori sanciti dalla Carta di Treviso e dal codice deontologico dei giornalisti. In particolare, ha ribadito che il rispetto delle garanzie poste a tutela dei minori riguarda anche il dovere di astenersi dal pubblicare stralci di atti processuali la cui diffusione potrebbe pregiudicarne la dignità (provv. 14 luglio 2014, n. 351, doc. web n. 3267450).

Video Pro Stamina

Il Garante ha adottato un provvedimento nei confronti di You-tube chiedendo di rimuovere un video pubblicato dal "Movimento Pro Stamina Italia" nel quale veniva ripresa, in modo da poter essere identificata, una bambina di quattro anni gravemente malata, con indebita diffusione di dati personali sensibili (provv. 18 gennaio 2014, n. 23, doc. web n. 2923201).

10.2. *La cronaca giudiziaria*

Informazioni relative a procedimenti

Sono stati esaminati dal Garante segnalazioni e reclami relativi al trattamento di dati personali nell'ambito della cronaca giudiziaria; ciò sempre in un'ottica di bilanciamento tra la tutela della riservatezza e della dignità delle persone e esigenze di

informazione e trasparenza sull'attività di amministrazione della giustizia, in attuazione dei principi di finalità, non eccedenza e proporzionalità del trattamento dei dati (note 30 giugno e 15 luglio 2014).

Vittime di reato

Come in passato, l'Autorità ha ribadito che, nella diffusione di notizie relative a procedimenti penali, particolare cautela deve essere adottata al fine di assicurare il diritto alla riservatezza e il rispetto della dignità delle persone offese da un reato. Ciò in considerazione del fatto che la pubblicità data a tale offesa può costituire per l'interessato un'ulteriore violazione dei propri diritti.

10.3. *I personaggi pubblici e l'utilizzo di artifici e raggiri*

Affrontando il tema della raccolta e della diffusione di informazioni riguardanti personaggi pubblici o che esercitano pubbliche funzioni – per i quali la diffusione di informazioni, pur se relative alla sfera privata, può risultare giustificata in ragione della "qualificazione del protagonista" (art. 6, comma 1, del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica), ovvero considerato il rilievo sul ruolo o sulla vita pubblica del soggetto cui le informazioni si riferiscono (art. 6, comma 2), ovvero, ancora, quando le medesime siano tratte da dichiarazioni o comportamenti pubblici degli interessati (art. 137, comma 3, del Codice) – il Garante ha ritenuto che non potesse essere diffuso il video che ritraeva un esponente politico, ritratto insieme ad alcuni pazienti, durante la sua permanenza all'interno di una casa di cura nella quale stava espiando la pena comminatagli attraverso l'affidamento al servizio sociale. Ciò considerato che il giornalista si era introdotto nella casa di cura, luogo non aperto al pubblico, senza dichiarare la propria identità, e aveva raccolto le immagini dell'interessato e dei pazienti ivi ricoverati mediante una microcamera ai fini della successiva diffusione, violando in tal modo le disposizioni relative alla correttezza nella raccolta dei dati (provv. 10 luglio 2014, n. 352, doc. web n. 3373321).

In altra vicenda l'Autorità ha intimato di non diffondere (nell'ambito di un noto programma televisivo) interviste fatte ad alcuni dipendenti del Senato, riprese con telecamera nascosta, che avevano consapevolmente rilasciato dichiarazioni a persone qualificatesi come giornalisti (ignari però delle riprese video ed audio) (cfr. nota 30 luglio 2014).

L'Ufficio ha altresì richiesto l'adesione spontanea ai principi normativi richiamati in una nota facente seguito ad una opposizione relativa ad una trasmissione televisiva nella quale veniva intervistato un noto attore, il quale aveva lamentato che il giornalista gli aveva rivolto domande su temi diversi da quelli concordati riguardanti la propria attività teatrale, come quello delle abitazioni private, in particolare concentrandosi sul mancato pagamento di alcuni canoni di locazione relativi ad un appartamento, oggetto di un provvedimento di sfratto. In particolare, l'Ufficio ha ritenuto che il giornalista aveva violato il principio di correttezza nell'esercizio dell'attività giornalistica e ha ottenuto la cancellazione spontanea del menzionato video dal sito web (nota 4 agosto 2014).

Esaminando la segnalazione con la quale un esponente politico ha lamentato un trattamento illecito di dati personali in relazione alla registrazione e alla successiva diffusione (durante una trasmissione radiofonica) della conversazione telefonica fatta con una persona che, imitando la voce di un altro esponente politico, lo aveva tratto in inganno circa la reale identità dell'interlocutore telefonico, il Garante ha ribadito il principio per cui il giornalista non può utilizzare artifici e raggiri per raccogliere notizie che potrebbero essere acquisite con gli strumenti propri dell'inchiesta

giornalistica (provv. 11 settembre 2014, n. 400, doc. web n. 3405138). Al riguardo il Garante ha rilevato che le modalità di raccolta dei dati del segnalante sono risultate in violazione dell'obbligo, sussistente in capo a chi effettua trattamenti a fini giornalistici, di rendere note le finalità della raccolta e, in particolare, di evitare l'uso di "artifici" (art. 2, comma 1, del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica).

Infine, il Garante ha ritenuto eccedente la pubblicazione su un quotidiano dell'indirizzo e della fotografia aerea dell'abitazione di un noto conduttore televisivo e ne ha vietato la diffusione, anche in considerazione del potenziale pregiudizio alla sicurezza dell'intervistato e della propria famiglia (provv. 11 settembre 2014, n. 399, doc. web n. 3471605).

10.4. *Gli archivi storici e le informazioni* online

In materia di informazioni *online*, ha suscitato un acceso dibattito e determinato rilevanti conseguenze pratiche la menzionata sentenza 13 maggio 2014 nel caso Google Spain, con la quale la Corte di giustizia ha stabilito che il gestore di un motore di ricerca su internet è titolare del trattamento dei dati personali che appaiono su pagine web pubblicate da terzi. La decisione è rilevante anzitutto perché estende la nozione di stabilimento prevista dall'art. 4, par. 1, lett. *a*), della direttiva 95/46/CE, ricomprendendo tra i trattamenti effettuati "nel contesto delle attività di uno stabilimento del responsabile (ndr. titolare per il Codice) di tale trattamento nel territorio di uno Stato membro" anche quelli posti in essere, in uno Stato membro, da una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da un motore di ricerca la cui attività si dirige agli abitanti di detto Stato membro.

Secondo la Corte, inoltre, il gestore di un motore di ricerca è "obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei *link* verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi" (anche quando la loro pubblicazione sia di per sé lecita). Questo obbligo si manifesta nel caso di dati inesatti, ma anche nel caso in cui "essi siano inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento, [...] non siano aggiornati, oppure [...] siano conservati per un arco di tempo superiore a quello necessario, a meno che la loro conservazione non si imponga per motivi storici, statistici o scientifici".

A parere della Corte di giustizia, il diritto ad ottenere la cancellazione dei *link* al proprio nome prevale, "in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse [del] pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi".

È da evidenziare che l'ampia interpretazione fornita dalla Corte di giustizia alla nozione di stabilimento ha consentito di applicare la disciplina di protezione dei dati di matrice europea anche ai trattamenti effettuati dai "giganti della rete", a prescindere dalla questione dell'interpretazione della nozione di "strumento/*equipment*" prevista dall'art. 4, par. 1, lett. *c*), della direttiva. Attribuire però ai gestori dei

motori di ricerca il compito di contemperare libertà di informazione e diritto alla protezione dei dati appare problematico, tenuto conto che tali soggetti possono non sempre essere dotati degli strumenti di conoscenza necessari per effettuare le (talora complesse) valutazioni nei singoli casi. In questo senso, di particolare rilievo rimane il ruolo che le autorità di protezione dei dati personali o le autorità giudiziarie nazionali competenti dovranno svolgere per contribuire ad un effettivo bilanciamento dei due diritti.

A seguito dell'appena richiamata sentenza della Corte di giustizia, Google è tenuta a dare un riscontro alle richieste di cancellazione dai risultati della ricerca delle pagine web che contengono il nominativo del richiedente (cfr. in merito le linee guida sull'attuazione della sentenza della Corte di giustizia nel caso Google Spain adottate dal Gruppo Art. 29 il 26 novembre 2014). La società dovrà valutare di volta in volta vari elementi, quali l'interesse pubblico a conoscere la notizia, il tempo trascorso dall'avvenimento nonché l'accuratezza della notizia e la rilevanza della stessa nell'ambito professionale di appartenenza. Di fronte al diniego di Google, gli utenti italiani possono rivolgersi al Garante o all'autorità giudiziaria.

In base a questa procedura, il Garante ha adottato alcuni provvedimenti a seguito delle prime segnalazioni pervenute dopo il mancato accoglimento da parte di Google di richieste di deindicizzazione di pagine presenti sul web che riportavano dati personali ritenuti non più di interesse pubblico. Le segnalazioni e i ricorsi pervenuti al Garante hanno riguardato la richiesta di deindicizzazione di articoli relativi a vicende processuali ancora recenti e in alcuni casi non concluse. In sette dei nove casi definiti, il Garante non ha accolto la richiesta degli interessati, ritenendo che la decisione di Google fosse corretta, risultando prevalente l'interesse pubblico ad accedere alle informazioni tramite motori di ricerca, tenuto conto che le vicende processuali erano recenti e non erano stati espletati tutti i gradi di giudizio (cfr. provv.ti 6 novembre 2014, n. 496, doc. web n. 3623819; n. 497, doc. web n. 3623954; n. 498, doc. web n. 3623919; n. 499, doc. web n. 623851; n. 500, doc. web n. 3623897; n. 558, doc. web n. 3624003 e n. 557, doc. web n. 3624021).

In due casi, invece, il Garante ha accolto la richiesta dei segnalanti, dando prevalenza alla tutela del loro diritto alla protezione dei dati (provv. 22 dicembre 2014, n. 501, doc. web n. 3623877 e provv. 11 dicembre 2014, n. 581, doc. web n. 3623978). Nel primo, perché nei documenti pubblicati su un sito web erano presenti numerose informazioni eccedenti, riferite anche a persone estranee alla vicenda giudiziaria narrata. Nel secondo, perché la notizia pubblicata era inserita in un contesto idoneo a ledere la sfera privata della persona. Tutto ciò in violazione delle norme del Codice e del codice deontologico che impongono ai giornalisti di diffondere dati personali nei limiti dell'"essenzialità dell'informazione riguardo a fatti di interesse pubblico" e di non riferire abitudini sessuali riferite a una determinata persona identificata o identificabile. Il Garante ha quindi prescritto a Google di deindicizzare l'url segnalata.

Va evidenziato che sono alcune decine, al momento, le segnalazioni pervenute all'Autorità a seguito della sentenza della Corte di giustizia: un numero esiguo, se paragonato alle 15.000 istanze rivolte finora a Google da cittadini italiani con le quali è stata richiesta la rimozione di circa 50.000 url. Rimozioni che la società ha accolto per il 25% dei casi (v. sul punto il rapporto di Google rinvenibile all'indirizzo http://www.google.com/transparencyreport/removals/europeprivacy/?hl=it).

11 Il trattamento di dati personali attraverso internet

11.1. *Informativa e consenso per il trattamento dei dati personali mediante i siti web*

L'Ufficio ha ravvisato informative sul trattamento dati non del tutto idonee ai sensi dell'art. 13 del Codice rispetto ad alcuni siti web nonché, rispetto a *form* di registrazione a servizi vari, consensi non adeguatamente differenziati a seconda dei diversi trattamenti di dati personali indicati nei testi informativi ai sensi degli artt. 23 e 130 del Codice.

In materia si segnala l'adozione del provv. 25 settembre 2014, n. 427 (doc. web n. 3457687), dal contenuto inibitorio e prescrittivo, adottato in relazione alla ricezione di messaggi promozionali indesiderati via *e-mail* da parte di utenti che avevano prestato il proprio consenso al solo scopo di ottenere l'iscrizione ad un servizio di *newsletter online*.

11.2. *Il provvedimento prescrittivo nei confronti di Google Inc.*

Si è conclusa con un provvedimento a carattere prescrittivo (10 luglio 2014, n. 353, doc. web n. 3283078) una complessa e rilevante istruttoria che ha preso in esame la *privacy policy* adottata da Google Inc., con particolare riguardo al trattamento di dati personali effettuato per finalità di profilazione *online*. La decisione, adottata nell'ambito di un'azione coordinata con altre autorità di protezione dati europee, non si è limitata a richiamare la società statunitense al rispetto dei principi fissati dal Codice, ma ha anche indicato in concreto le misure e le modalità da adottare per rendere leciti i trattamenti effettuati, in particolare in materia di informativa, consenso e tempi di conservazione dei dati. In considerazione delle complessità, anche dal punto di vista tecnico, delle misure necessarie per dare attuazione alle prescrizioni, alla società è stato concesso un termine di diciotto mesi per l'adeguamento, nel corso del quale il Garante potrà monitorare tale processo avvalendosi di uno specifico protocollo di verifica concernente tempi e modalità dei controlli da parte dell'Autorità.

11.2.1. Google Street View Special Collects

Google Inc. ha comunicato all'Autorità l'intenzione di estendere al territorio nazionale un programma, già attivo altrove, di "raccolta immagini in luoghi unici e remoti, inclusi quelli con particolare valore naturalistico, storico e turistico", denominato *Google Special Collects*.

Al riguardo, ed in considerazione del campo di applicazione della raccolta di immagini in questione – riservata a luoghi (privati, pubblici ed aperti al pubblico) di particolare interesse artistico, turistico, storico e culturale che, per le loro caratteristiche strutturali, risultano accessibili esclusivamente a piedi o, comunque, con mezzi diversi dall'automobile –, l'Autorità, riconosciute le peculiarità del servizio rispetto alla versione *standard* di *Street View*, ha individuato adeguate cautele a tutela degli interessati e misure semplificate per informarli delle riprese (programmate o in corso). In particolare, Google dovrà rendere noti i luoghi oggetto di ripresa sul proprio sito web in italiano nei tre giorni antecedenti l'inizio delle riprese nonché, sette

giorni prima, anche sui siti web e, se esistenti, sulle *newsletter* o altre pubblicazioni informative dei *partners*, cioè degli enti, strutture, soggetti privati, fondazioni, ecc. coinvolti nel programma. Nei luoghi ad accesso controllato, Google o i suoi incaricati dovranno rendere nota alle persone interessate – anche attraverso appositi avvisi o cartelli affissi all'ingresso dei siti – l'imminente registrazione delle immagini, in modo da minimizzare il rischio per i visitatori che non lo desiderano di venire ripresi.

La società dovrà inoltre provvedere alla formazione del personale coinvolto circa il rispetto della normativa sulla protezione dei dati personali e dotare gli operatori di adesivi o altri segni distintivi chiaramente visibili da applicare sull'abbigliamento e sulle attrezzature, in modo da segnalare che si stanno acquisendo immagini da pubblicare *online* su *Google maps* mediante il servizio *Google Special Collects* nell'ambito di *Street View* (provv. 4 dicembre 2014, n. 555, doc. web n. 3633473).

11.3. *La raccolta dati* online *da siti specializzati per richieste di preventivi di prestiti*

Anche a seguito delle segnalazioni pervenute, l'Autorità ha avviato un'attività di verifica sul trattamento dei dati effettuati mediante siti web riferiti a consumatori nel settore delle domande di prestito personale e di altre modalità di finanziamento (in corrispondenza, ad esempio, della cd. cessione del quinto, dell'acquisto dell'auto o del "mutuo prima casa") con l'obiettivo di verificare la liceità dei trattamenti, anche alla luce delle Linee guida in materia di attività promozionale e contrasto allo *spam* (provv. 4 luglio 2013, n. 330, doc. web n. 2542348) ed il corretto impiego delle informazioni raccolte in sede di ricerca di possibili finanziamenti.

A seguito di tale attività il Garante ha adottato due provvedimenti inibitori e prescrittivi (provv.ti 9 ottobre 2014, n. 447, doc. web n. 3568046 e 20 novembre 2014, n. 532, doc. web n. 3657934). Nel primo caso, ha vietato ad una società di intermediazione *online* l'utilizzo dei dati personali dei clienti a fini di *marketing* in assenza di un loro consenso specifico. In particolare, a seguito di una segnalazione in cui si lamentava la ricezione di comunicazioni promozionali indesiderate, è stato accertato che la società sottoponeva agli utenti un modello di richiesta di consenso unico (ritenuto inidoneo), peraltro già pre-compilato nella casella relativa all'assenso, sia per la fornitura del servizio richiesto, sia per finalità diverse, quali l'invio di informazioni commerciali e la fidelizzazione della clientela. Il Garante ha inoltre prescritto di modificare e integrare l'informativa presente sul sito, al fine di rendere chiaramente noti agli utenti i trattamenti di dati effettuati, le modalità di svolgimento dell'attività promozionale per conto proprio o da parte di soggetti terzi nonché l'eventuale comunicazione a terzi dei dati.

Con il secondo provvedimento, valutate le informazioni presenti sul sito e previo accertamento *ex* art. 157 del Codice, il Garante ha dichiarato illecita e vietato la raccolta dei dati personali degli utenti effettuata da una società sul sito web per l'invio di comunicazioni promozionali per conto proprio e per conto terzi nonché di comunicazione dei dati raccolti a terzi per finalità promozionali (o comunque per finalità diverse da quelle strumentali ovvero collegate all'erogazione del servizio o all'esecuzione del contratto) senza aver provveduto alla previa acquisizione del necessario consenso libero e specifico degli interessati, oltre che informato e documentato per iscritto (art. 23, comma 3, del Codice); ha inoltre prescritto alla medesima società di modificare la formula di acquisizione del consenso nonché di specificare nell'informativa le modalità tradizionali (posta cartacea, telefonate con operatore) e/o automatizzate (posta elettronica, sms, fax) di utilizzazione dei dati per lo svolgimento dell'attività promozionale.

11.4. *L'attività istruttoria condotta dall'Autorità a seguito di accertamenti ispettivi del Nucleo speciale* privacy *e di segnalazioni*

È stata intensificata l'attività di verifica sulla conformità al Codice dei trattamenti effettuati da talune società editoriali in occasione della raccolta dei dati degli utenti sui rispettivi siti web; ciò con specifico riferimento all'informativa resa e alle modalità di acquisizione del consenso al trattamento dei dati (artt. 13, 23 e 130 del Codice) nonché ai fondamentali principi di finalità, necessità, proporzionalità e non eccedenza del trattamento (artt. 3-11 Codice). La complessa attività ha interessato principalmente editori oggetto di accertamenti ispettivi da parte del Nucleo speciale *privacy* della Guardia di finanza (nell'ambito del programma delle attività ispettive del primo semestre 2012) nei confronti dei quali erano stati individuati, già in sede ispettiva, profili di illiceità rispetto a taluni trattamenti determinando così l'avvio di procedimenti sanzionatori.

Tale approfondimento si è reso necessario in considerazione dell'abitualità della raccolta dei dati in questo ambito, spesso finalizzata al perseguimento di plurime finalità (consultare il giornale *online*; acquistare un abbonamento; ricevere *newsletter*; esprimere commenti sulle notizie, partecipare a *blog* e *forum* su temi di attualità) nonché considerata la complessità della struttura organizzativa dei titolari del trattamento (spesso strutturati in gruppi societari), con riflessi sull'ambito di circolazione nonché sulle modalità e finalità di utilizzo dei dati raccolti. L'Autorità ha quindi verificato non solo la "regolarizzazione" dei trattamenti alla luce delle contestazioni formulate in sede ispettiva, ma ha altresì esteso la verifica alle diverse attività di raccolta dei dati effettuate dagli editori attraverso i propri siti. Ciò anche alla luce dei provvedimenti generali in materia di *spam* (cfr. provv. 4 luglio 2013, n. 330, doc. web n. 2542346) e sul consenso al trattamento dei dati personali per finalità di *marketing* diretto (cfr. provv. 15 maggio 2013, n. 242, doc. web n. 2543820).

Fra i profili critici emersi si segnala che, nell'informativa e nello spazio dedicato all'acquisizione del consenso, tra le finalità ulteriori rispetto a quelle connesse alla prestazione del servizio richiesto, spesso è stato riscontrato il riferimento ad "attività statistiche e di sondaggio di opinioni" finalizzate anche a un "miglioramento del servizio richiesto". Tale formulazione ha reso necessario un chiarimento sulle effettive finalità (statistica aggregata/profilazione) perseguite dall'editore, essendo talvolta richiesti all'utente anche dati eccedenti rispetto a quelli necessari all'erogazione del servizio (di navigazione sul sito *web* o di accesso a determinati contenuti), in particolare con riferimento a dati concernenti professione, età, titolo di studio, sesso. Inoltre, in alcune informative è risultata mancare l'indicazione di un indirizzo *e-mail* dedicato all'esercizio gratuito e, per quanto possibile, agevole dei diritti di cui agli artt. 7 ss. del Codice, come suggerito dal Gruppo Art. 29 (cfr. parere n. 5/2004) e ribadito dalle citate Linee guida del 4 luglio 2013.

L'Autorità ha fatto presente a ciascun titolare che, in base all'art. 11, comma 2, del Codice, i dati personali raccolti in violazione della disciplina non avrebbero comunque potuto essere utilizzati per finalità promozionali, né avrebbero potuto essere comunicati a terzi per analoghe finalità, se non dopo aver raccolto un libero consenso informato e specifico per ciascuno di questi trattamenti, ai sensi degli artt. 13, 23 e 130 del Codice.

11.5. *L'utilizzo dei* cookie*: adozione del provvedimento generale*

Nella Relazione 2013 sono state descritte le modalità, improntate a criteri di ampia partecipazione, attraverso le quali l'Autorità ha acquisito, sia mediante consultazione pubblica sia mediante predisposizione di un apposito tavolo di lavoro, i contributi provenienti dalla comunità tecno-scientifica ed imprenditoriale sull'uso dei cd. *cookie* (i piccoli *file* di testo che i siti visitati dall'utente inviano al suo *browser* per essere poi ritrasmessi agli stessi siti alla successiva visita del medesimo utente) e di altri strumenti analoghi (quali *web beacon/web bug, clear* GIF). Ciò ha consentito di appurare che l'impiego dei *cookie* nell'ambito della navigazione in internet, se da un lato consente la profilazione degli utenti tesa all'invio di pubblicità mirata, dall'altro assicura anche il funzionamento dei servizi offerti *online*.

Alla luce degli elementi raccolti, con provvedimento generale dell'8 maggio 2014, n. 229 (doc. web n. 3118884), il Garante ha individuato modalità semplificate per rendere agli utenti l'informativa *online* e ha fornito indicazioni per acquisirne il consenso, quando richiesto, nonché per consentire agli interessati di decidere in maniera libera e consapevole se autorizzare l'uso delle informazioni personali inerenti la propria navigazione attraverso i siti visitati per ricevere pubblicità mirata. A maggior tutela degli utenti, il Garante ha stabilito che quando si accede alla *home page* o ad un'altra pagina di un sito web deve comparire un *banner* chiaramente visibile, in cui sia indicato:

- se il sito utilizza *cookie* di profilazione per inviare messaggi pubblicitari mirati;
- se il sito consente anche l'invio di *cookie* di "terze parti", ossia di *cookie* installati da un titolare del trattamento diverso rispetto a quello che gestisce il sito visitato;
- un *link* a una informativa più ampia, recante indicazioni sull'uso dei *cookie* inviati dal sito con le indicazioni necessarie a negare il consenso alla loro installazione direttamente o collegandosi ai vari siti nel caso dei *cookie* di "terze parti";
- l'indicazione che proseguendo nella navigazione (ad es., accedendo ad un'altra area del sito ovvero selezionando un'immagine o un *link*) si presta il consenso all'uso dei *cookie*.

Per quanto riguarda l'obbligo di tener traccia del consenso dell'utente, al gestore del sito è consentito utilizzare un *cookie* tecnico, in modo tale da non riproporre l'informativa breve alla seconda visita dell'utente, il quale conserva comunque la possibilità di modificare le proprie scelte sui *cookie* attraverso l'informativa estesa, che deve essere facilmente accessibile da ogni pagina del sito.

Il termine per l'implementazione delle misure prescritte è fissato per maggio 2015.

12 Il trattamento di dati personali nel settore delle comunicazioni elettroniche

12.1. *Il* telemarketing *"selvaggio"*

Per quanto riguarda le utenze iscritte al Registro pubblico delle opposizioni continua a pervenire un ingente numero di segnalazioni relative alla ricezione di chiamate promozionali indesiderate. Numerose segnalazioni hanno riguardato altresì telefonate a carattere commerciale effettuate nei confronti di utenze – fisse e mobili – non presenti negli elenchi telefonici (cd. utenze riservate) come pure di utenze, non riservate e non iscritte nel Registro pubblico delle opposizioni, per le quali è stato negato il consenso al trattamento dei dati personali nei confronti di una o più società (che, ciò nonostante, hanno effettuato le chiamate promozionali).

Parallelamente all'esame delle segnalazioni sono proseguite le complesse attività istruttorie volte ad individuare l'effettivo autore della chiamata indesiderata ed a riscontrare la presenza o meno di uno specifico consenso al trattamento dei dati personali da parte del segnalante. Il fenomeno delle chiamate indesiderate dirette a numeri presenti in elenco ha spesso comportato la necessità di acquisire informazioni direttamente dalla Fondazione Ugo Bordoni.

Sono ben 735 le comunicazioni – comprensive di richieste d'informazioni (anche *ex* art. 157 del Codice), richieste d'integrazione di istruttorie e note volte a verificare l'avvenuto adeguamento alla disciplina di protezione dei dati – inviate alle società segnalate od alla Fondazione Ugo Bordoni. Sono inoltre circa 100 le note inviate ai segnalanti per informarli sullo stato della propria pratica ovvero per richiedere informazioni integrative. In numerosi casi, peraltro, si è constatato che le aziende che hanno svolto attività a contenuto promozionale hanno operato anche tramite terzi i quali, a loro volta, hanno ulteriormente demandato l'attività promozionale ad altri soggetti, talora stabiliti all'estero. Lo svolgimento dell'attività istruttoria ha comportato altresì la necessità di svolgere un previo accertamento sulla titolarità delle utenze segnalate. In un sempre crescente numero di casi, tuttavia, il numero chiamante è risultato oscurato ovvero solo apparentemente in chiaro (in quanto, ricontattando l'utenza telefonica, la stessa è risultata essere "inesistente").

Sono state trattate un totale di 1.398 pratiche, delle quali, per più di 1.000, è stata conclusa l'attività istruttoria. In più di 80 casi, inoltre, l'attività è stata definita con la trasmissione degli atti al Dipartimento competente per l'apertura di un procedimento sanzionatorio. Gli accertamenti svolti nell'ambito delle istruttorie, peraltro, hanno determinato in taluni casi la necessità di effettuare attività di carattere ispettivo nei confronti sia dei soggetti committenti l'attività di *telemarketing*, sia di alcuni *call center* che le hanno materialmente poste in essere.

12.2. *Le nuove regole di contrasto alle telefonate mute effettuate da* call center *per finalità di* marketing

Il Garante ha continuato ad occuparsi del fenomeno delle chiamate mute, vale a dire delle telefonate promozionali nelle quali, a causa dell'arbitraria e non corretta

impostazione dei sistemi automatizzati di chiamata utilizzati dai *call center*, il destinatario, dopo aver risposto, non trova dall'altro capo del filo alcun operatore. Riguardo tale fenomeno, a seguito della consultazione pubblica avviata a fine novembre 2013, il Garante ha adottato il provvedimento 20 febbraio 2014, n. 83 (doc. web n. 3017499) indicando una serie di misure di contrasto. Con tale decisione, in particolare, si è stabilito che:

- i *call center* devono censire correttamente e secondo criteri uniformi le chiamate mute effettuate, che devono comunque essere interrotte entro un massimo di 3 secondi dalla risposta dell'utente;
- 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*;
- alla risposta dell'utente non potrà 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, ecc., per dare la sensazione che la chiamata non provenga da molestatori;
- a seguito di una chiamata muta, l'utente non potrà essere ricontattato prima di cinque giorni e comunque al contatto successivo dovrà essere prevista una modalità di instradamento automatico della chiamata in modo da assicurare la presenza di un operatore;
- i *call center* dovranno conservare per almeno due anni i *report* statistici delle chiamate mute effettuate, in modo da consentire gli opportuni controlli.

Il termine per l'adeguamento di sei mesi è scaduto il 2 ottobre 2014. Al riguardo, l'Autorità ha in programma di svolgere un'attività di carattere ispettivo al fine di verificare la conformità dei trattamenti di dati personali effettuati dai *call center* alle prescrizioni impartite.

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

A seguito delle prescrizioni impartite con il provvedimento del 10 ottobre 2013, n. 444 (doc. web n. 2724806), sono pervenute al Garante, da parte di quarantuno titolari del trattamento, le notificazioni di trasferimento o affidamento all'estero del trattamento di dati personali per servizi di *call center*. L'Autorità ha così potuto iniziare ad effettuare una ricognizione più completa del fenomeno acquisendo elementi utili a verificare la conformità alle prescrizioni impartite dal suddetto provvedimento ed alle disposizioni del Codice anche mediante accertamenti ispettivi, in collaborazione con il Nucleo speciale *privacy* della Guardia di finanza, per verificare la liceità dei trattamenti posti in essere dai titolari che si avvalgono di *call center* esteri.

12.4. *Dati personali utilizzati a fini di* marketing *e profilazione*

È stata presentata all'Autorità, ai sensi dell'art. 17 del Codice e del provvedimento generale del 24 febbraio 2005 relativo alle carte di fidelizzazione (doc. web n. 1103045), un'istanza di verifica preliminare da parte di una società che effettua crociere che aveva richiesto di poter conservare i dati della propria clientela per finalità di profilazione e *marketing* per un periodo pari a tredici anni rilevando che, per

poter effettuare una minima attività di profilazione, si sarebbe dovuto prendere in considerazione un numero di crociere sostenute dallo stesso passeggero pari a tre e che l'arco temporale indicato sarebbe stato congruo per tale finalità. Il Garante, con il provvedimento di accoglimento del 12 giugno 2014, n. 297 (doc. web n. 3315156), ricordando che tali attività necessitano comunque, preliminarmente, del consenso degli interessati, ha stimato congruo un periodo di conservazione massimo pari a dieci anni. Sempre con il medesimo provvedimento è stato altresì prescritto, allo scadere del suddetto termine di dieci anni, l'obbligo di cancellazione automatica dei dati conservati ovvero la trasformazione degli stessi in forma anonima in modo permanente.

Si deve evidenziare che, rispetto ai trattamenti svolti 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 del previsto consenso specifico come stabilito nel provvedimento generale del 25 giugno 2009 (doc. web n. 1629107) e a seguito dei provvedimenti individuali emananti in tale ambito all'esito delle verifiche preliminari richieste da ciascun fornitore, il Garante ha adottato, a fronte di un'apposita istanza di riesame ed aggiornamento presentata da uno degli operatori telefonici coinvolti, uno specifico provvedimento prescrittivo (provv. 6 febbraio 2014, n. 54).

Al contempo, l'Autorità ha aggiornato le prescrizioni precedentemente impartite (provv. 6 febbraio 2014, n. 53, doc. web n. 2951718) rivedendo la misura prescrittiva che stabiliva un tempo di osservazione dei dati personali aggregati degli utenti per finalità di profilazione non inferiore ai trenta giorni. Ciò in virtù della prospettata esigenza, di fronte ad un nuovo assetto del mercato delle telecomunicazioni, di considerare, dopo alcuni anni dall'emanazione del provvedimento del 2009 e dei singoli provvedimenti prescrittivi, una nuova e più ridotta base temporale di aggregazione dei dati per finalità di profilazione, così da garantire un maggior equilibrio nei processi di gestione della clientela, soprattutto in ragione del crescente ricorso da parte degli utenti allo strumento della *number portability* e della crescente "offerta dati" legata alla diffusione di dispositivi radiomobili evoluti, quali *smartphone* e *tablet.*

In questo quadro il Garante ha previsto una riduzione del periodo di osservazione da un arco temporale mensile ad uno di due giorni, prescrivendo al contempo nuove cautele a garanzia degli utenti. Tra queste, l'Autorità ha disposto che la misurazione dei fenomeni che rilevano per l'attività di profilazione, sulla base di una aggregazione dei dati degli utenti relativa al suddetto arco temporale, debba riguardare esclusivamente: il volume di minuti in traffico originato o terminato (in minuti o *byte*); il numero di eventi di ricarica, distinto per canale di ricarica; il totale delle ricariche.

Limitatamente ai dati relativi al volume di minuti in traffico originato o terminato, il Garante ha inoltre previsto l'esclusione dall'impiego per finalità di profilazione dei periodi a cui corrisponda un solo evento di comunicazione elettronica riferibile ad un singolo utente.

Nel provvedimento si è altresì precisato che per tutte le altre misurazioni, ovvero per l'analisi aggregata dei dati che riguardano altri eventi che il fornitore individua per finalità di profilazione della clientela, quali i contatti dell'utente con il *customer care*, le visite ai diversi punti vendita ed assistenza del fornitore nonché le offerte relative ai terminali, la base temporale minima di riferimento debba essere di trenta giorni.

12.5. *I trattamenti dei dati personali per finalità di* marketing *diretto: manifestazione del consenso*

Nel caso di un noto gruppo societario l'Ufficio, dopo aver verificato che i dati del segnalante erano inseriti nelle liste dei soggetti contattabili per finalità di *marketing* diretto in assenza del necessario consenso, ha provveduto a trasmettere la relativa documentazione al competente Dipartimento ai fini dell'eventuale avvio di appositi procedimenti sanzionatori (nota 11 novembre 2014). In tale occasione si è ribadito che l'invio di comunicazioni pubblicitarie, anche con modalità automatizzate di contatto, deve essere effettuato nel rispetto delle norme che disciplinano i trattamenti in ambito privato a fini promozionali (artt. 23 e 130, commi 1 e 2, del Codice).

L'Autorità è intervenuta anche con riguardo ai profili della comunicazione a soggetti terzi e del trasferimento all'estero dei dati personali nell'ambito della stipula di contratti di assicurazioni per la responsabilità civile degli autoveicoli. In tali ipotesi è stato ribadito che, pur potendosi accettare l'acquisizione del consenso per finalità di *marketing* in calce al testo dell'informativa rilasciata al cliente e la successiva "premarcatura" in calce al contratto di assicurazione successivamente sottoscritto in quanto riproposizione di un consenso già rilasciato, non è invece da ritenersi ammissibile un consenso unico per finalità di *marketing* e di comunicazione a terzi (nota 23 dicembre 2014).

Il Garante è intervenuto in materia di manifestazione del consenso al trattamento per finalità promozionali anche con due provvedimenti inibitori e prescrittivi (provv. 9 gennaio 2014, n. 3, doc. web n. 2904350; provv. 25 settembre 2014, n. 427, doc. web n. 3457687). A seguito di segnalazioni inerenti alla ricezione di messaggi promozionali indesiderati via *e-mail*, l'Ufficio ha avviato altrettante istruttorie dalle quali è emerso che le stesse erano state inviate da società che avevano acquisito il consenso degli interessati in maniera non conforme al Codice, non essendo lo stesso libero e specifico.

In un caso infatti, la società titolare aveva raccolto il consenso al trattamento dei dati personali all'atto della sottoscrizione da parte dell'interessato di un modulo per l'attivazione della garanzia su un prodotto richiedendo un unico consenso per tutte le finalità (comprese quelle promozionali) indicate nella sua informativa; pertanto all'interessato non era lasciata la possibilità di esprimere liberamente la propria volontà in riferimento ad ogni distinta finalità di trattamento perché, in mancanza di consenso, non era possibile accedere al servizio. Nell'altro caso, invece, la stessa modalità di raccolta del consenso era stata utilizzata per richiedere l'iscrizione ad un servizio di *newsletter online*.

In entrambi i casi, il Garante, con i summenzionati provvedimenti, ha dichiarato illecito il trattamento effettuato per finalità promozionali poiché il consenso prestato dagli interessati non era libero e specifico ed ha vietato l'ulteriore trattamento dei dati così acquisiti avviando, al contempo, altrettanti procedimenti sanzionatori.

12.6. *Il* mobile payment

Facendo seguito all'attività conoscitiva svolta nel 2013 in merito ai nuovi servizi di pagamento attraverso il telefono cellulare, il Garante ha adottato, dopo una preliminare fase di consultazione pubblica (avviata il 12 dicembre 2013), un provvedimento generale in materia di trattamento di dati personali nell'ambito dei servizi di *mobile remote payment* (provv. 22 maggio 2014, n. 258, doc. web n. 3161560),

volto a delineare un primo quadro organico di regole, senza penalizzare lo sviluppo del mercato digitale.

Le misure previste hanno riguardato numerosi soggetti tra cui, in particolare, operatori di telecomunicazioni, *hub* tecnologici e fornitori di beni e servizi digitali fruibili tramite *smartphone*, *tablet* e *pc*, ma anche quanti offrono agli utenti la possibilità di acquistare, tramite applicazioni che consentono l'accesso a un mercato virtuale, contenuti digitali grazie al *mobile payment*. In questo ambito il provvedimento ha definito diversi profili, fra cui: le modalità per fornire l'informativa agli utenti e i suoi contenuti; le modalità per manifestare il consenso da parte degli interessati; la sicurezza e conservazione dei dati trattati.

In particolare, con riguardo all'informativa è stato chiarito che, oltre al richiamo alla finalità di erogazione del servizio attraverso la nuova modalità *mobile payment*, la stessa deve specificare se i dati personali dell'utente sono trattati anche per scopi ulteriori (quali *marketing* o profilazione) o comunicati a terzi, richiamando la necessità dell'acquisizione dell'apposito consenso dell'interessato.

In questo ambito, peraltro, sono state indicate le modalità di manifestazione del consenso, anche rispetto all'eventuale trattamento di dati sensibili. Infatti, il Garante ha evidenziato che, qualora dalla fruizione del contenuto o del servizio digitale sia possibile dedurre informazioni di natura sensibile, il consenso dell'interessato deve essere manifestato per iscritto, ovvero con altra modalità telematica equiparabile allo scritto, nel rispetto di quanto previsto dall'art. 26, comma 1, del Codice. Nella medesima ottica, la modalità telematica equiparabile allo scritto può implicare, oltre al ricorso ad un documento sottoscritto con firma elettronica qualificata o digitale, anche il ricorso a forme alternative più diffuse, secondo quanto previsto dal menzionato d.P.R. n. 445/2000. In ogni caso è possibile per il titolare del trattamento individuare forme alternative di manifestazione del consenso in luogo di quelle previste dalla normativa, soggette alla valutazione del Garante ai sensi dell'art. 17 del Codice.

L'Autorità ha prescritto nuove misure volte a garantire la sicurezza dei dati, quali sistemi di autenticazione forte per l'accesso ai dati da parte del personale, procedure di tracciamento degli accessi e delle operazioni effettuate, criteri di codificazione dei prodotti e servizi, forme di mascheramento dei dati.

Altre misure sono state individuate anche al fine di evitare i rischi di una integrazione tra le diverse tipologie di dati a disposizione dell'operatore telefonico (consumo/traffico telefonico e dati relativi alla fornitura di altri beni digitali, quali ad esempio quelli legati alla cd. tv interattiva) e impedire quindi un'eventuale profilazione incrociata dell'utenza rispetto alle abitudini, ai gusti ed alle preferenze di consumo, in assenza del relativo consenso espresso, specifico e informato.

Anche per i *merchant* (i fornitori di contenuti digitali offerti agli utenti, quali copie digitali di quotidiani, *social games*, *e-book*, contenuti musicali e video), nella prospettiva di garantire la maggiore riservatezza dei dati dei clienti, è stata prevista la trasmissione all'operatore telefonico delle sole categorie merceologiche di riferimento dei prodotti digitali offerti, senza indicazioni sullo specifico contenuto del prodotto o servizio acquistato, a meno che ciò non sia in concreto necessario per la fornitura di servizi in abbonamento.

Altri accorgimenti hanno riguardato la previsione di apposite misure di sicurezza per la fruizione di servizi destinati ad un pubblico adulto, nonché la conservazione dei dati trattati.

Successivamente, in accoglimento dell'istanza interpretativa e di riesame di alcune prescrizioni contenute nel provvedimento suindicato presentata da un'associazione rappresentativa del settore e della successiva istanza di proroga del termine di attuazione previsto dal provvedimento stesso, l'Autorità (cfr. provv. 20 novembre 2014,

n. 546, doc. web n. 3610915) ha prorogato il termine al 31 marzo 2015, fornendo altresì indicazioni interpretative (classificazione dei contenuti; misure di sicurezza; periodo di conservazione dei dati).

12.7. *Il contrasto allo* spam

Numerose continuano ad essere le segnalazioni relative a sms, fax e (ancor più) *e-mail* indesiderati: nel coltivarle, non di rado risulta difficile individuare i titolari del trattamento, per le modalità con cui si può operare in rete, sia perché talora i siti mittenti risultano intestati a soggetti di fantasia o comunque privi di recapiti utilmente contattabili, sia perché spesso essi hanno sede in Paesi (anche extraeuropei) ove l'Autorità non ha competenza (v. art. 5 del Codice).

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

Con riguardo ai fax indesiderati si segnala il provvedimento del 23 gennaio 2014, n. 30 (doc. web n. 2927848), a tutela delle persone giuridiche, il quale ha ribadito che le disposizioni normative del capo 1 del titolo X del Codice, e in particolare quelle sulle modalità automatizzate di contatto promozionale (*e-mail*; *sms*; fax; *mms*; telefonate preregistrate), poiché riguardano i "contraenti", tutelano non solo le persone fisiche ma anche persone giuridiche, enti e associazioni. Quindi, ad ordinamento vigente, i titolari del trattamento dei dati relativi ai detti soggetti sono sottoposti al potere dell'Autorità di intervenire anche *ex officio* nonché all'applicazione delle sanzioni ammnistrative e penali previste dal Codice (e, tra queste, dall'art. 162, comma 2-*bis*) (v. provv. 20 settembre 2012, doc. web n. 2094932, e, analogamente, punto 2.2, Linee guida 4 luglio 2013, n. 330, doc. web n. 2542348). Peraltro, è stato chiarito che sono "dati personali" anche quelli relativi a professionisti e ad alcune imprese, come ad esempio per le persone fisiche che gestiscono ricevitorie o tabaccherie o agenzie di viaggio, in quanto tali soggetti sono da ritenersi "interessati" ai sensi dell'art. 4 del Codice. Inoltre, è stato precisato che l'invio di un fax è già in sé un trattamento di dati personali, indipendentemente dall'eventuale successivo inserimento dei dati del destinatario in un elenco *online* o comunque accessibile al pubblico, che costituisce un ulteriore distinto trattamento; dal numero dei fax eventualmente inviati al destinatario della promozione, bastando anche un solo fax indesiderato per integrare un trattamento di dati illegittimo; dall'informativa sul trattamento resa al destinatario ai sensi dell'art. 13 del Codice; dall'avviso del titolare ai destinatari delle promozioni indesiderate riguardo ai diritti di cui agli artt. 7 ss. del Codice; dal fatto che i dati in questione vengano cancellati subito dopo l'invio indesiderato in caso di mancata risposta o di opposizione dei destinatari. È stato ribadito che, senza il consenso libero e specifico dell'interessato, non è possibile trattare i dati "tratti da registri pubblici, elenchi, siti web, atti o documenti conosciuti o conoscibili da chiunque" (v. punto 2.5, Linee guida 4 luglio 2013).

12.8. *Servizi di TV digitale: non è* spam

È stata esaminata una segnalazione che lamentava la ricezione di messaggi pubblicitari indesiderati, associati alla visione di programmi offerti da un operatore telefonico nell'ambito dei servizi di tv digitale, che non sono assimilabili alle modalità di contatto automatizzato di cui all'art. 130, commi 1 e 2, del Codice.

Al riguardo, tuttavia, è emerso che i messaggi di cui si lamentava la ricezione non avevano natura pubblicitaria, trattandosi di *video-clip* di breve durata tesi esclusivamente ad informare l'utente circa i contenuti audiovisivi disponibili, a cui l'apposito *decoder*, installato per la ricezione del servizio televisivo digitale terrestre, consentiva l'accesso, nonché la possibilità per l'utente di bloccare tale ricezione attraverso due diverse modalità funzionali. In considerazione di ciò, l'Ufficio non ha ravvisato i presupposti per l'applicabilità della normativa sulla protezione dei dati personali.

12.9. *Le notificazioni di avvenuti* data breach

Sono pervenute all'Autorità ventidue comunicazioni di *data breach*, formulate dai più importanti fornitori di servizi di comunicazione elettronica operanti in Italia. La maggior parte delle violazioni notificate ha riguardato la perdita accidentale di documentazione contrattuale pur essendo sempre presente una copia dei dati in formato elettronico acquisita sui sistemi dei titolari. In alcuni casi, la violazione ha riguardato i servizi offerti *online* dai fornitori sui propri siti web, come quelli che consentono ai clienti di effettuare ricariche telefoniche o visualizzare il traffico telefonico effettuato a fini di controllo dell'esattezza degli addebiti. Gli incidenti hanno determinato la visualizzazione, da parte di alcuni clienti, dei dati relativi ad altri interessati.

In tali vicende, 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 assicurandosi, al contempo, che gli interessati fossero stati informati dagli operatori nei casi previsti. Non si è ritenuto necessario adottare uno specifico provvedimento; in un solo caso la violazione non è stata prontamente notificata dalla società per difetto di qualificazione del reclamo ricevuto da un cliente il quale però, nel frattempo, aveva segnalato l'evento al Garante e dato impulso ad un'apposita istruttoria; è stato così rilevato il mancato rispetto, da parte del fornitore, dei ristretti termini previsti 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 avviato un separato procedimento sanzionatorio.

Accanto alla gestione ordinaria delle comunicazioni di *data breach*, l'Autorità ha seguito gli approfondimenti svolti a livello europeo, partecipando ad una serie di incontri con le altre autorità competenti in ambito comunitario. I temi di maggiore rilievo affrontati hanno riguardato la collaborazione tra le diverse autorità nazionali competenti, la valutazione delle misure tecnologiche di protezione adottate dai fornitori, con particolare riferimento all'inintelligibilità dei dati, per far fronte alle singole violazioni e l'introduzione di eventuali ipotesi di esenzione dall'obbligo di notificazione.

12.10. Data retention

È proseguita l'analisi delle risultanze del ciclo ispettivo effettuato dal Nucleo speciale *privacy* in materia di conservazione di dati di traffico telefonico e telematico (cfr. Relazione 2013, *passim*), come noto oggetto della sentenza della Corte di giustizia dell'8 aprile 2014 (Digital Rights Ireland e Seitlinger e a., cause riunite C-293/12 e C-594/12) con la quale la Corte ha dichiarato invalida la direttiva sulla conservazione dei dati di traffico ritenendo che dalla stessa derivi un'ingerenza di ampia portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati (cfr. par. 23.3).

Tali accertamenti, avviati nel 2012 a seguito di delibera del Collegio, erano stati effettuati nei confronti di vari fornitori di comunicazione elettronica accessibili al pubblico di piccole e medie dimensioni. Ciò al fine di verificare il rispetto delle prescrizioni impartite dal Garante con il provvedimento generale del 17 gennaio 2008 concernente la sicurezza dei dati di traffico telefonico e telematico, successivamente integrato con un secondo provvedimento generale del 24 luglio 2008, resosi necessario in virtù del recepimento della direttiva 2006/24/CE (cd. direttiva Frattini), riguardante "la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione", avvenuto con il d.lgs. 30 maggio 2008, n. 109, che ha modificato, tra l'altro, l'art. 132 del Codice (cfr. doc. web nn. 1482111 e 1538237).

All'esito di tale attività è stato adottato il provv. 20 febbraio 2015, n. 84 (doc. web n. 3031194) grazie al quale è stata prescritta al fornitore l'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 tenuta di un apposito registro degli accessi. È stato altresì prescritto di svolgere, con cadenza almeno annuale, un'attività di controllo interna adeguatamente documentata e di procedere, entro il medesimo termine, alla cancellazione dei dati di traffico relativi alle chiamate senza risposta conservati oltre il termine di trenta giorni previsto dall'art. 132, comma 1-*bis*, del Codice.

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

Il trattamento dei dati personali connesso all'attuazione delle discipline in materia di trasparenza amministrativa, oggetto delle "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" (provv. 15 maggio 2014, n. 243, doc. web n. 3134436), è stato uno dei profili sui quali si è focalizzata l'attenzione del Garante in ambito lavorativo; ma non può non rilevarsi il persistere di un significativo interesse per la materia della videosorveglianza in relazione alla quale l'Autorità è stata investita da numerose istanze di intervento. L'ambito di utilizzo delle tecnologie di localizzazione nel contesto lavorativo si è andato estendendo anche ai dispositivi mobili quali gli *smartphone* forniti in dotazione ai dipendenti: in particolare il Garante è stato chiamato a pronunciarsi sulle condizioni di liceità delle applicazioni informatiche che consentono la localizzazione dei lavoratori.

Rappresentatività sindacale nel settore privato

Con riguardo al tema della misura della rappresentatività sindacale nel settore privato, ai fini della contrattazione nazionale di categoria, di particolare rilievo il parere reso su richiesta dell'Istituto nazionale della previdenza sociale (Inps) avente ad oggetto uno schema di convenzione tra l'Istituto e Confindustria, Cgil, Cisl e Uil al fine di verificare la rappresentatività dei sindacati, così come previsto dal "Testo unico sulla rappresentanza" sottoscritto il 10 gennaio 2014. Esaminata la bozza di convenzione, l'Autorità ha sottolineato che, per misurare la rappresentatività sindacale, non è necessaria la trasmissione da parte delle imprese all'Inps dei dati sensibili, concernenti l'affiliazione sindacale, riferiti a ciascun lavoratore, in quanto lo stesso fine è perseguibile mediante la sola rilevazione del mero numero di deleghe assegnate a ciascuna sigla sindacale (parere 18 dicembre 2014, n. 609, doc. web n. 3721603). In linea con quanto espresso dal Garante, in data 16 marzo 2015 è stata quindi stipulata la menzionata convenzione nella quale si prevede la raccolta da parte dell'Inps dei soli dati numerici concernenti le deleghe riferite a ciascuna sigla sindacale. Tali dati numerici saranno successivamente trasmessi al Cnel per lo svolgimento delle operazioni di ponderazione e di determinazione della misura della rappresentatività di ciascuna sigla sindacale stipulante la convenzione.

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

Videosorveglianza

L'esame della casistica che ha formato oggetto di provvedimenti collegiali in materia di rapporti di lavoro, anche a seguito di accertamenti ispettivi, conferma che in relazione all'utilizzo di strumenti di controllo, in particolare di sistemi di videosorveglianza, si riscontra un'area significativa di trattamenti non conformi, oltre che alla disciplina di settore (art. 4, l. n. 300/1970), anche alla disciplina sul trattamento dei dati personali (artt. 11, comma 1, lett. *a*), e 114 del Codice).

L'inosservanza della disciplina vigente in materia è stata accertata, unitamente alla violazione delle disposizioni che impongono di informare compiutamente sia i dipendenti che i terzi (in particolare clienti e fornitori) circa le caratteristiche essenziali dei sistemi di videosorveglianza installati, in relazione a titolari del trattamento

che svolgono attività eterogenee, in particolare quella relativa al settore alberghiero (provv. 9 gennaio 2014, n. 13, doc. web n. 2927804), alla grande distribuzione (provv. 8 maggio 2014, n. 230, doc. web n. 3250490) e ai piccoli esercizi commerciali (provv.ti 18 settembre 2014, n. 412, doc. web n. 3500271 e 4 dicembre 2014, n. 559, doc. web n. 3671057).

È stata altresì riscontrata l'inosservanza dell'obbligo di effettuare la designazione degli incaricati del trattamento e, in caso di affidamento dei servizi di vigilanza a soggetti esterni (svolti, ad es., tramite accesso alla *control room* dove vengono visualizzate in tempo reale le immagini raccolte con le telecamere di sorveglianza oppure mediante installazione di sistemi di allarme gestiti da remoto contestualmente al monitoraggio delle immagini), della designazione di questi ultimi quali responsabili del trattamento (provv.ti 9 gennaio 2014, n. 13 e 4 dicembre 2014, n. 559, cit.). Tali adempimenti, previsti dagli artt. 29 e 30 del Codice, sono finalizzati individuazione di soggetti realmente idonei a trattare i dati personali conformemente alla disciplina vigente, in base alle specifiche istruzioni predisposte dal titolare del trattamento.

Il Garante ha anche precisato che i dati personali riferiti ai dipendenti trattati attraverso un sistema di videosorveglianza installato per finalità di sicurezza e di tutela dei beni aziendali non possono essere utilizzati per contestare illeciti disciplinari (provv. 2 ottobre 2014, n. 434, doc. web n. 3534543). Tale utilizzo per scopi ulteriori e diversi rispetto a quelli originariamente perseguiti si pone in contrasto sia con il principio di finalità del trattamento (art. 11, comma 1, lett. *b*), del Codice) che con la disciplina vigente in materia di controlli a distanza dei lavoratori (cfr. provv. 8 aprile 2010, doc. web n. 1712680, punto 4.1; v. in merito anche le puntualizzazioni formulate a seguito di una verifica preliminare relativa ad un sistema di videosorveglianza cd. intelligente presso la Banca d'Italia riferite al par. 4.8).

Si segnala inoltre che l'Autorità – in occasione della richiesta avanzata da una società del settore metalmeccanico – ha chiarito che l'installazione di telecamere all'interno degli spogliatoi aziendali viola i principi di liceità, necessità, pertinenza e non eccedenza (posti dagli artt. 3 e 11, comma 1, lett. *a*), del Codice). Infatti all'interno di tali aree l'intimità e la dignità dei dipendenti devono essere indefettibilmente tutelate, anche alla luce delle vigenti disposizioni dell'ordinamento civile e penale, come già affermato in precedenza (provv. 10 luglio 2014, n. 357, doc. web n. 3325380).

Geolocalizzazione

Quanto all'utilizzo delle tecnologie di localizzazione in ambito lavorativo, tema già oggetto di un provvedimento di carattere generale con riferimento alla geolocalizzazione di veicoli (provv. 4 ottobre 2011, n. 370, doc. web n. 1850581), il Garante si è pronunciato sulle condizioni di liceità dell'utilizzo di applicazioni informatiche che consentono di localizzare geograficamente dispositivi mobili (*smartphone*) forniti in dotazione ai dipendenti. In particolare, nell'ambito di verifiche preliminari richieste da due importanti società di telecomunicazioni, l'Autorità ha ritenuto che il trattamento di dati personali riferiti alla localizzazione di dispositivi che – differentemente dai veicoli di servizio – da un lato "seguono" costantemente il dipendente, dall'altro si prestano ad utilizzi anche privati (nel caso considerato, peraltro, consentiti dal datore di lavoro), presenta rischi specifici per le libertà (ad es., di circolazione e di comunicazione), i diritti e la dignità dei lavoratori (v. provv.ti 11 settembre 2014, n. 401, doc. web n. 3474069 e 9 ottobre 2014, n. 448, doc. web n. 3505371). L'utilizzo dei sistemi – finalizzato al perseguimento di finalità organizzative e di sicurezza del lavoro nonché configurato in modo tale da non consentire la rilevazione continuativa dei dati – è stato pertanto subordinato all'adozione di misure di tipo organizzativo e tecnologico volte ad impedire l'eventuale trattamento da parte del datore di lavoro di informazioni presenti sul dispositivo estranee alla finalità di gestione del rapporto di lavoro (ad es., riferite a sms, traffico telefonico, posta elettronica, naviga-

zione in internet) e a rendere edotti i dipendenti in tempo reale (attraverso un'apposita icona sullo schermo dello *smartphone*) dell'attivazione della funzionalità di localizzazione. È stata data inoltre applicazione alla disciplina sul cd. bilanciamento di interessi (cfr. art. 24, comma 1, lett. *g*), del Codice), considerato anche che i titolari del trattamento hanno attivato le procedure previste dalla disciplina in materia di controlli a distanza dei dipendenti (previste dall'art. 4, comma 1, l. n. 300/1970) ed hanno dichiarato che i dati relativi alla posizione geografica non verranno utilizzati per finalità disciplinari.

Anche in relazione ai dati relativi alla posizione geografica, come nell'ambito della videosorveglianza, il Garante ha ritenuto che l'eventuale utilizzo per fini disciplinari di sistemi installati per scopi organizzativi, produttivi o legati alla sicurezza del lavoro non sarebbe conforme sia al principio di finalità del trattamento (art. 11, comma 1, lett. *b*), del Codice) che alla disciplina vigente in materia di controlli a distanza dei lavoratori, anch'essa applicabile (provv. 2 ottobre 2014, n. 434, cit.).

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

L'Autorità continua a ricevere numerose segnalazioni e reclami relativi a forme di accesso ad informazioni personali oppure a modalità di circolazione delle stesse all'interno della struttura lavorativa, ritenute indebite, tanto nel settore pubblico che nel settore privato.

A tale proposito il Garante, nel confermare che il personale che svolge specifiche mansioni di segreteria in base ad un atto di preposizione può legittimamente curare la consegna di comunicazioni al dipendente di una amministrazione pubblica (nel caso specifico con qualifica dirigenziale) nell'ambito di un procedimento disciplinare, quanto alle modalità di consegna delle stesse ha ritenuto altresì lecito l'utilizzo dell'indirizzo di posta elettronica istituzionale assegnato al dipendente contestualmente alla consegna a mano in busta chiusa (all'interno della stanza assegnata al dipendente stesso). È stata invece ritenuta non conforme al principio di pertinenza e non eccedenza l'invio di copia di una contestazione disciplinare ad una articolazione interna dell'ufficio sprovvista di competenze relative al procedimento disciplinare (provv. 31 luglio 2014, n. 392, doc. web n. 3399423).

In un altro caso, con riguardo al trattamento dei dati personali dei dipendenti posto in essere da un gestore del servizio di trasporto pubblico, consistente nella affissione sulle bacheche ubicate presso i depositi aziendali (nonché tramite la rete aziendale intranet), di tabelle relative ai turni di servizio degli autisti, il Garante ha chiarito che sebbene le informazioni concernenti le causali di assenza dei lavoratori possano lecitamente essere oggetto di trattamento da parte del datore di lavoro – mediante il personale espressamente incaricato ai sensi dell'art. 30 del Codice –, nella misura in cui siano necessarie e pertinenti per dare corretta esecuzione al rapporto di lavoro ovvero per attuare previsioni contenute in leggi, regolamenti, contratti e accordi collettivi (artt. 11 comma 1, lett. *a*) e *d*), nonché 24, lett. *a*) e *b*) e, con riferimento ai dati sensibili, art. 26 del Codice e autorizzazione n. 1/2013, relativa al trattamento dei dati sensibili nei rapporti di lavoro) tuttavia, le medesime informazioni, specie se di natura sensibile, non possono essere messe a conoscenza di terzi non legittimati e degli altri dipendenti addetti al servizio di trasporto. Il Garante, sebbene non abbia ritenuto sussistente nel caso di specie, un'ipotesi di diffusione ai sensi dell'art. 4, comma 1, lett. *m*), del Codice – atteso che le tabelle erano state rese disponibili al personale in una sezione ad accesso riservato della intranet aziendale e su bacheche ubicate in locali il cui accesso era consentito unicamente ad

un novero determinato o determinabile di soggetti (art. 4, comma 1, lett. *l*), del Codice) –, ha tuttavia rilevato che l'espressa indicazione di numerose informazioni di dettaglio sulle ragioni giustificative dell'assenza dal servizio con riguardo a ciascun lavoratore, ancorché mediante sigle sintetiche, acronimi o abbreviazioni, rende indebitamente edotto ciascun lavoratore di vicende personali riferite ad altri colleghi, dando luogo ad un'illecita comunicazione di dati personali (provv. 3 luglio 2014, n. 341, doc. web n. 3325317).

Ancora in tema di circolazione di informazioni all'interno della struttura lavorativa, in questo caso privata, in occasione della lamentata illecita comunicazione ad una pluralità di soggetti (tra i quali la quasi totalità dei colleghi appartenenti all'unità organizzativa di appartenenza del segnalante) di dati personali anche sensibili contenuti in un ricorso presentato davanti all'autorità giudiziaria e notificato al datore di lavoro (tra i quali specifiche patologie e relative terapie), il Garante ha prescritto di conformare il sistema di protocollazione informatica ai principi di protezione dei dati personali. Posto che nel caso concreto è risultata accertata l'inesistenza di alcuna procedura differenziata e/o riservata preordinata alla gestione di dati anche sensibili contenuti in atti giudiziari nell'ipotesi – tutt'altro che remota, soprattutto in relazione a società di grandi dimensioni – in cui gli atti stessi siano riferiti a dipendenti della società, il trattamento effettuato è stato ritenuto illecito per violazione dei principi di necessità, pertinenza e non eccedenza (provv. 12 giugno 2014, n. 298, doc. web n. 3318492).

Nell'ambito del rapporto di lavoro pubblico, con riferimento alla comunicazione di dati personali effettuata via telefono dal responsabile del personale al medico che ha redatto certificazioni relative ad un dipendente, il Garante ha chiarito che l'attività volta a far valere i diritti dell'amministrazione in relazione a certificazioni mediche ritenute non veritiere deve essere svolta utilizzando gli strumenti di controllo già previsti dalla disciplina di settore anche al fine di prevenire o contrastare condotte assenteistiche (che non contemplano, allo stato, attività di accertamento svolte direttamente nei confronti di colui che redige la certificazione sanitaria) nonché, se del caso, rivolgendosi alla competente autorità giudiziaria. Anche in occasione della tutela di propri diritti – che comunque deve svolgersi con modalità conformi ai principi di pertinenza e non eccedenza rispetto alle finalità perseguite – il datore di lavoro pubblico può, infatti, comunicare dati personali del dipendente solo se ciò sia previsto da una norma di legge o di regolamento (provv. 10 aprile 2014, n. 187, doc. web n. 3214369).

Merita evidenziare che in un altro caso il Garante ha ritenuto invece non fondata la segnalazione concernente il trattamento di dati sensibili da parte di un'amministrazione comunale nell'ambito di attività "dirette all'accertamento della responsabilità civile, disciplinare e contabile [...]" del lavoratore (cfr. artt. 11, comma 1, lett. *a*), 20, comma 1 e art. 112, comma 2, lett. *g*), del Codice), confermando che, al fine di far valere i propri diritti in relazione a fenomeni di assenteismo e di eventuale non veritiera certificazione sanitaria, è possibile redigere note informative, segnalazioni o denunce contenenti anche riferimenti circostanziati alle ragioni e alle modalità delle singole assenze alle competenti istituzioni (cfr. punto 8.2, 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, doc. web n. 1417809; v. anche provv. 24 settembre 2001, doc. web n. 39460). Nel caso di specie il datore di lavoro aveva richiesto al competente Ordine provinciale dei medici, nel rispetto della disciplina di settore (cfr. art. 5, l. n. 300/1970, artt. 55 e ss., d.lgs. n. 165/2001; sul punto, v. anche Dipartimento della funzione pubblica, Circolare n. 7 del 12 novembre 2009), "un controllo sulle certificazioni sanitarie prodotte" dall'interessato al

fine di giustificare le proprie assenze per malattia derivante da causa di servizio. Tanto, in presenza di un particolare comportamento tenuto dal dipendente, documentato dalla certificazione attestante la specifica consecuzione dei periodi di assenza per malattia, rispetto al quale, in ragione delle peculiarità del caso concreto, non potevano essere esperiti gli ordinari strumenti di controllo sulle assenze (cfr. art. 2 comma 1, lett. *c*), d.m. 18 dicembre 2009, n. 206 che esclude dall'obbligo di rispettare le fasce di reperibilità i dipendenti per i quali l'assenza è dovuta a malattie per le quali sia stata riconosciuta la causa di servizio) (provv. 5 giugno 2014, n. 281, doc. web n. 3275942).

Anche il tema della liceità della comunicazione da parte di un soggetto pubblico in qualità di datore di lavoro alle organizzazioni sindacali di dati personali concernenti i lavoratori (quali nominativi, emolumenti percepiti ovvero numero di ore di straordinario effettuato dai singoli lavoratori) è stato oggetto di attenzione da parte del Garante che ha reso un proprio parere all'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (Aran). In particolare, la richiesta di chiarimenti formulata dall'Agenzia concerneva la legittimità dell'istanza avanzata da parte di alcune organizzazioni sindacali nei confronti della dirigenza scolastica volta ad ottenere, in applicazione del Contratto collettivo nazionale del "comparto scuola" (art. 6, comma 2 del Ccnl 29 novembre 2007), i "nominativi del personale utilizzato nelle attività e progetti retribuiti con il fondo d'istituto" nonché "i compensi erogati individualmente" a ciascuno di essi. Nel prendere atto che, in base ad alcune disposizioni contenute nei contratti collettivi applicabili per i singoli comparti dell'amministrazione, determinate informazioni in materia di gestione del rapporto di lavoro possono essere oggetto di specifici diritti di informazione (preventiva o successiva) in favore delle parti sindacali, il Garante ha affermato che solo ove il contratto collettivo applicabile preveda espressamente che l'informazione sindacale abbia ad oggetto anche dati nominativi del personale è possibile procedere a siffatta comunicazione (cfr. in particolare, punto 5.2. prima parte delle Linee guida, provv. 14 giugno 2007, doc. web n. 1417809). Nei restanti casi è consentita "solamente la comunicazione in forma anonima" (cfr. sul punto, provv. 20 dicembre 2012, n. 431, doc. web n. 2288474; in senso analogo, v. anche provv. 18 luglio 2013, n. 358, doc. web n. 2578201 che, con riguardo a specifici casi, hanno confermato le indicazioni già fornite in via generale con le menzionate Linee guida). Nel prendere posizione con riguardo allo specifico caso relativo al "comparto scuola", è stato pertanto chiarito che le norme contrattuali di riferimento consentono la comunicazione dei nominativi dei docenti coinvolti nelle attività finanziate con il cd. fondo d'Istituto (art. 6, comma 2, lett. *n*), Ccnl cit.), non già la comunicazione dei compensi accessori erogati individualmente i quali potranno essere comunicati indicandone l'importo complessivo "per fasce" o "qualifiche". Da ultimo il Garante, nel ribadire che restano impregiudicate le altre forme di conoscibilità degli atti amministrativi, nei limiti e con le modalità stabilite dalla disciplina di settore (artt. 22 ss., legge 7 agosto 1990, n. 24; sulla legittimazione all'esercizio del diritto di accesso da parte delle organizzazioni sindacali cfr. C.d.S., Sez. VI, 20 novembre 2013, nn. 6186 e 5511, ma anche C.d.S., Sez. VI, 23 febbraio 2012, n. 1034 e 11 gennaio 2010, n. 26, da ultimo, Tar Emilia Romagna, Sez. Parma, 28 maggio 2014, n. 173), ha precisato che la messa a disposizione di terzi delle citate informazioni non può comunque avvenire attraverso la diffusione sul sito web dell'istituto scolastico, atteso che la recente disciplina in materia di trasparenza prevede di dare evidenza dei livelli di selettività e premialità nella distribuzione dei premi e degli incentivi al personale "in forma aggregata" (art. 20, commi 1 e 2, d.lgs. n. 33/2013) (nota 7 ottobre 2014).

In tema di comunicazione di dati personali relativi al trattamento economico dei dipendenti e collaboratori, l'Autorità – in risposta ad un quesito formulato dal Ministero dell'economia e delle finanze – ha ritenuto che il testo dell'art. 60, comma 3, d.lgs. 20 marzo 2001, n. 165, come modificato dall'art. 2, d.l. 31 agosto 2013, n. 101 (convertito con modificazioni in l. 30 ottobre 2013, n. 125), debba essere interpretato nel senso che le società partecipate dalle pubbliche amministrazioni nonché tutti gli altri soggetti indicati dalla norma (e in particolare, tra questi, la società concessionaria del servizio pubblico radiotelevisivo) sono tenute a comunicare alla Presidenza del Consiglio dei ministri – Dipartimento della funzione pubblica nonché al Ministero dell'economia e delle finanze, informazioni relative al costo annuo del personale rese anche in forma non nominativa ed eventualmente aggregate per tipologia contrattuale e classi stipendiali. La citata norma, inoltre, non contempla alcuna forma di pubblicazione di dati personali nominativi riferiti ai singoli rapporti di lavoro (nota 27 marzo 2014).

13.3. *La pubblicazione* online *dei dati personali riferiti ai dipendenti*

In più occasioni il Garante è stato chiamato a pronunciarsi sulla pubblicazione *online* sui siti istituzionali degli enti pubblici ovvero nell'ambito delle sezioni dedicate all'albo pretorio, di dati, atti o provvedimenti contenenti dati personali riferiti a lavoratori – già oggetto di precedenti pronunce e da ultimo del menzionato provvedimento generale del 15 maggio 2014, n. 243, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati (*in merito v.* par. 4.4) – accertando in molti casi l'illiceità del trattamento per violazione della disciplina di settore (ad es., con riguardo alla mancata osservanza dei termini massimi di pubblicazione) ovvero per mancata osservanza del principio di pertinenza e non eccedenza rispetto alle spesso invocate finalità di validità e completezza della motivazione ovvero di adempimento agli obblighi dettati in materia di pubblicità legale degli atti amministrativi.

In particolare, a fronte della lamentata pubblicazione di deliberazioni sul sito web di un comune, il Garante ha ribadito, nel solco di precedenti decisioni, che la diffusione di dati personali mediante la pubblicazione di atti e relativi allegati, può essere lecitamente effettuata da parte di un soggetto pubblico unicamente quando tale operazione sia prevista da una norma di legge o di regolamento (artt. 11, comma 1, lett. *a*), e 19, comma 3, del Codice). Nel caso considerato è stata riscontrata l'illiceità della diffusione di atti rimasti consultabili sul sito del comune oltre l'arco temporale previsto dalla disciplina di settore (cfr. art. 124, d.lgs. 18 agosto 2000, n. 267 concernente la pubblicità degli atti degli enti locali sull'albo pretorio, nonché art. 32, l. 18 giugno 2009, n. 69). L'illiceità è stata rilevata anche alla luce del principio di pertinenza e non eccedenza (art. 11, comma 1, lett. *d*), del Codice), in considerazione del fatto gli stessi riportavano valutazioni e giudizi riguardanti l'operato del lavoratore nell'esecuzione della propria prestazione lavorativa (provv. 13 marzo 2014, n. 121, doc. web n. 3112708).

In alcuni casi ha formato oggetto di segnalazione la pubblicazione di graduatorie concorsuali o altri atti contenenti dati riferiti alle condizioni di invalidità di centinaia di lavoratori o partecipanti alle prove concorsuali, sovente unitamente ad altre informazioni (agevolmente raggiungibili mediante i comuni motori di ricerca) in alcuni casi eccedenti (ad esempio, il codice fiscale ed ulteriori informazioni concernenti titoli di preferenza) ed immediatamente visibili in rete tramite l'inserimento delle

generalità degli interessati nei più diffusi motori di ricerca generalisti. In alcuni casi le graduatorie recavano in chiaro i dati identificativi degli interessati nell'ambito di procedure selettive pubbliche riservate "ai soggetti disabili di cui alla legge n. 68/1999 (provv.ti 6 marzo 2014, n. 109, doc. web n. 3039272; 19 giugno 2014, n. 313, doc. web n. 3259444). In altro caso si trattava invece della diffusione di una delibera di un ente locale che disponeva il collocamento a riposo di un dipendente per "inabilità assoluta e permanente a qualsiasi proficuo lavoro" (cfr. art. 2, l. 12 giugno 1984, n. 222 e art. 13, l. 8 settembre 1991, n. 274, nonché, art. 2, comma 12, l. 8 agosto 1995, n. 335) (nota 20 giugno 2014). È stata altresì lamentata la diffusione sui siti web di istituti scolastici e di uffici periferici del Ministero dell'Istruzione, dell'Università e della Ricerca di graduatorie relative al personale docente, contenente dati non pertinenti (quali, il codice fiscale e il numero di figli a carico) ma anche dati relativi alle condizioni di salute degli interessati; in particolare, in allegato alle menzionate graduatorie docenti risultavano pubblicati gli elenchi di decine di docenti "riservisti" e "disabili art. 1, l. n. 68/99", che dava conto della fruizione da parte del personale dei benefici derivanti dall'art. 21, l. 5 febbraio 1992, n. 104 (con riguardo alla precedenza nell'assegnazione della sede per le persone con gravi invalidità) e dall'art. 61, l. n. 20 maggio 1982, n. 270 (che disciplina modalità di assegnazione della sede e titoli di preferenza per gli insegnanti non vedenti) (provv. 25 settembre 2014, n. 426, doc. web n. 3505289). In tutti i casi il Garante ha ribadito l'illiceità della diffusione di dati da cui si possa desumere lo stato di salute dei soggetti interessati (art. 22, comma 8, del Codice), compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici, disponendo il divieto dell'ulteriore diffusione in Internet di tali dati personali e prescrivendo l'adozione da parte del titolare del trattamento di idonei accorgimenti nelle operazioni di trattamento (cfr. quanto da ultimo previsto dal già citato provv. 15 maggio 2014, n. 243, doc. web n. 3134436; v. anche, tra i tanti, provv. 10 ottobre 2013, n. 442, doc. web n. 2753605 e nello stesso senso, con riferimento alla diffusione di determinazioni aventi ad oggetto la liquidazione di indennizzi per patologie contratte per causa di servizio, provv. 22 novembre 2012, n. 362, doc. web n. 2194472).

Quesiti in materia di trasparenza e anticorruzione

Al fine di fornire prime indicazioni con riguardo ai profili derivanti dall'applicazione della normativa in materia di protezione dei dati nell'ambito dell'osservanza degli obblighi di pubblicità degli atti amministrativi e di quelli stabiliti dalla recente normativa in materia di trasparenza, il Garante ha fornito riscontro a specifiche richieste di parere o quesiti formulati dalle pubbliche amministrazioni e altri soggetti istituzionali.

Permessi sindacali *online*

In particolare il Garante si è pronunciato in riscontro ad un quesito formulato dalla Presidenza del Consiglio dei ministri - Dipartimento della funzione pubblica avente ad oggetto la pubblicazione dei nominativi dei dipendenti fruitori di permessi, distacchi ed aspettative sindacali, rilevando in primo luogo che la diffusione di tali dati personali idonei rivelare l'affiliazione sindacale degli interessati (ai sensi dell'art. 4, comma 1, lett. *d*), del Codice) può essere effettuata solo se autorizzata da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite (art. 20, comma 1, del Codice). Il trattamento delle stesse è ammesso per le esigenze connesse alla gestione del rapporto di lavoro nell'ambito dell'adempimento di specifici obblighi o compiti previsti dalla normativa "in materia sindacale" (cfr. art. 112, comma 2, lett. *e*), del Codice) e in conformità al d.P.C.M. 30 novembre 2006, n. 312 (Regolamento concernente il trattamento dei dati sensibili e giudiziari presso la Presidenza del Consiglio dei ministri) adottato ai sensi dell'art. 20, comma 2, del Codice, con atto di natura regolamentare (previo

parere espresso dal Garante). Il quadro normativo di riferimento richiede un flusso informativo da parte delle pp.aa. al Dipartimento della funzione pubblica dei dati relativi all'appartenenza sindacale al solo fine della predisposizione della Relazione annuale al Parlamento sullo stato della p.a. e prevede la sola pubblicazione in forma aggregata di tali informazioni ai sensi dell'art. 16, l. 29 marzo 1983, n. 93 oltre che, al fine di consentire il monitoraggio della spesa per le prerogative sindacali nel settore pubblico, anche alla Corte dei conti (art. 50, d.lgs. 30 marzo 2001, n. 165, nonché art. 4, comma 4, d.m. 23 febbraio 2009). Pertanto il Garante ha concluso che, non trovando applicazione al caso di specie le norme contenute nella recente disciplina in materia di trasparenza (d.lgs. 14 marzo 2013, n. 33), la diffusione in internet dei dati nominativi dei fruitori dei permessi non è prevista dalla legge e risulta una misura sproporzionata in una società democratica (cfr. sul punto anche art. 8, par. 1, direttiva 95/46/CE e altresì *Article 29 Data Protection Working Party, Advice paper on special categories of data (sensitive data)*, 4 aprile 2011) rispetto alla finalità dell'efficace controllo sulla fruizione delle prerogative sindacali nell'ambito del pubblico impiego, finalità peraltro già perseguita mediante la banca dati Gedap costituita presso il Dipartimento della funzione pubblica (provv. 16 gennaio 2014, n. 15, doc. web n. 2922911).

È stato altresì esaminato il caso sottoposto dal Ministero dell'interno avente ad oggetto la legittimità della richiesta, avanzata da parte di una delle organizzazioni sindacali rappresentative della carriera prefettizia, di pubblicare sul sito istituzionale del dicastero la proposta di graduatoria in esito al procedimento di valutazione comparativa dei funzionari per il passaggio alla qualifica di viceprefetto. Secondo la ricostruzione del quadro normativo operata dall'Autorità, impregiudicate le altre forme di conoscibilità e pubblicità delle graduatorie e degli altri atti riguardanti i concorsi, le prove selettive e le progressioni di carriera previste dall'ordinamento, l'art. 23, comma 1, lett. *c*), d.lgs. n. 33/2013 – su cui gli istanti fondavano la richiesta di pubblicazione – non può costituire idonea base normativa per la diffusione di tali atti sul sito istituzionale del Ministero. La norma prevede, infatti, la pubblicazione, con aggiornamento semestrale, sul sito web delle pp.aa, in apposite partizioni della sezione "Amministrazione trasparente", nella forma di una scheda sintetica, dei soli "elenchi" dei provvedimenti finali (non anche gli atti intermedi del procedimento) relativi anche a "concorsi e prove selettive"; inoltre, per ciascuno dei provvedimenti finali compresi nei menzionati elenchi sono pubblicati esclusivamente "il contenuto, l'oggetto, l'eventuale spesa prevista e gli estremi relativi ai principali documenti contenuti nel fascicolo relativo al procedimento" (nota 9 maggio 2014).

Con riguardo alla richiesta avanzata da parte di una testata giornalistica mirante a conoscere il trattamento pensionistico del segretario generale cessato dall'incarico e degli *ex* dipendenti dell'Assemblea regionale siciliana è stato chiarito che la disciplina del Codice non può essere invocata per negare, in via di principio, l'accesso ai documenti anche da parte degli organi di stampa, salva in ogni caso la responsabilità del giornalista in ordine alla diffusione del dato raccolto secondo i parametri dell'essenzialità, della correttezza, della pertinenza e della non eccedenza, avuto altresì riguardo alla natura del dato medesimo (cfr. Chiarimenti all'Ordine dei giornalisti del 6 maggio 2004, doc. web n. 1007634; artt. 136, 137 e 138 del Codice; codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica, All. A1 al Codice). Il Garante ha tuttavia precisato che, con riguardo alla diversa disciplina in materia di trasparenza, resta salva la facoltà in capo alle pubbliche amministrazioni di disporre la pubblicazione di documenti ulteriori, non individuati dal d.lgs. n. 33/2013 o da altra specifica norma di legge o di regolamento (art. 19, comma 3, del Codice), "procedendo alla anonimizzazione dei dati personali

eventualmente presenti" (art. 4, comma 3, d.lgs. n. 33/2013, nonché, parte I, punto 3, provv. 15 maggio 2014, n. 243, doc. web n. 3134436) (nota 9 giugno 2014).

L'Anac, nell'ambito di una più ampia consultazione pubblica, ha sottoposto al Garante per proprie osservazioni la bozza della delibera che, estendendo, in alcuni casi, la portata di una disposizione normativa dalla formulazione lacunosa, disciplina il regime di trasparenza delle dichiarazioni sulla insussistenza delle cause di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e altri enti privati in controllo pubblico, ai sensi dell'art. 20, d.lgs. 8 aprile 2013, n. 39 (Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico a norma dell'art. 1, commi 49 e 50, della legge 6 novembre 2012, n. 190). La predetta disposizione – all'interno di un testo normativo (il d.lgs. n. 39/2013, appunto) che stabilisce una casistica minuziosa di ipotesi di inconferibilità e incompatibilità (sulla scorta dei criteri e dei principi già enucleati nella legge di delega, l. 6 novembre 2012, n. 190) – è disposizione in materia di trasparenza che va comunque coordinata con i principi, di derivazione comunitaria, a tutela del diritto alla riservatezza e alla protezione dei dati personali. In particolare, secondo l'Autorità il predetto art. 20 introduce nuovi obblighi di "pubblicazione obbligatoria" volti a conseguire finalità di trasparenza il cui adempimento, ove comporti la diffusione di informazioni riferite a persone identificate o identificabili, deve avvenire nel rispetto dei principi di protezione dei dati personali (cfr. art. 1, comma 2, nonché, artt. 4, 6, 8 comma 3, d.lgs. n. 33/2013) (nota 14 aprile 2014).

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

Il Garante si è pronunciato con riguardo alle istanze formulate ai sensi degli artt. 19 comma 2 e 39 del Codice. In particolare, un'azienda sanitaria cui è funzionalmente assegnato personale, docente e non docente, di un'università in base ad un apposito protocollo d'intesa, aveva chiesto all'ateneo l'elenco degli iscritti al sindacato. Tanto al fine di accertare l'effettiva adesione al sindacato che aveva agito per il pagamento di alcune competenze economiche in favore dei propri iscritti. Poiché tali dati sono idonei a rivelare l'appartenenza sindacale dei lavoratori (art. 4, comma 1, lett. *d*), del Codice), il loro trattamento può essere effettuato da parte dei soggetti pubblici in presenza di espressa disposizione di legge nella quale siano specificati, non solo i tipi di dati che possono essere trattati e la natura delle operazioni eseguibili, ma anche le finalità di rilevante interesse pubblico perseguite (art. 20, comma 1, del Codice). Sebbene la richiesta finalità di rilevante interesse pubblico, nel caso di specie, poteva essere ricondotta nelle esigenze connesse alla gestione del rapporto di lavoro – in particolare nell'adempimento degli "obblighi retributivi" di cui all'art. 112, comma 2, lett. *d*), del Codice –, tuttavia i regolamenti per il trattamento dei dati sensibili e giudiziari adottati ai sensi dell'art. 20, comma 2, del Codice dai due enti interessati non prevedono tale particolare ipotesi di comunicazione. Per tali ragioni, il Garante ha valutato di non poter autorizzare siffatta comunicazione, salvo, in ogni caso, l'eventuale aggiornamento dei regolamenti previo parere del Garante (art. 20 comma 2, del Codice). Né sarebbe stato possibile applicare al caso di specie la procedura semplificata prevista agli artt. 19, comma 2 e 39, commi 1, lett. *a*), del Codice, atteso che tale disciplina opera per la comunicazione da parte dei soggetti pubblici dei soli dati personali diversi da quelli sensibili. Tale procedimento, contemperando le esigenze di semplificazione e speditezza dell'azione amministrativa, quando sia volta a soddisfare necessità connesse all'esercizio di pubbliche

funzioni, con il principio di legalità e tassatività dei casi di comunicazione dei soli dati comuni (art. 19, comma 2, del Codice), subordina all'obbligo di comunicazione al Garante la possibilità, in assenza di eventuali e anche successive determinazioni dello stesso, di porre in essere la comunicazione dei dati in favore di altro soggetto pubblico. In particolare, l'attività di comunicazione dei dati comuni "da parte di un soggetto pubblico ad altri soggetti pubblici" è ammessa solamente quando sia espressamente prevista da "una norma di legge o di regolamento" (art. 19, comma 2, del Codice); in mancanza di tale base giuridica la comunicazione può essere utilmente intrapresa, quando sia comunque necessaria per lo svolgimento di funzioni istituzionali, decorsi 45 giorni dalla comunicazione al Garante – chiamato a verificare se tali funzioni siano effettivamente realizzabili, in base al quadro normativo vigente, unicamente attraverso l'acquisizione dei dati richiesti – e in assenza di "diversa determinazione" dello stesso (artt. 19, comma 2 e 39, comma 2, del Codice) (provv. 31 luglio 2014, n. 394, doc. web n. 3394281).

Analoga richiesta ai sensi degli artt. 19, comma 2 e 39, comma 1, lett. *a*), del Codice è stata formalizzata da un altro ateneo per comunicare dati, in prevalenza anagrafici, del personale universitario ad un'azienda ospedaliero-universitaria che svolge funzioni di assistenza, didattica e ricerca nell'ambito del Servizio sanitario nazionale e del sistema universitario e che intendeva realizzare un sistema di gestione della sicurezza e salute sul lavoro sia con riguardo al proprio personale che con riguardo a quello di dipendenza universitaria che opera presso le proprie strutture sanitarie. Nell'ambito di un'attività di monitoraggio della *performance* dei processi relativi alla formazione e alla ricerca si chiedevano, inoltre, i dati relativi alle attività didattiche, alle pubblicazioni di coloro che lavorano in ambito aziendale e quelli infine connessi ai prodotti ed esiti dell'attività di ricerca (quali pubblicazioni, brevetti, ecc.). Il Garante ha valutato che la disciplina in materia di tutela della salute e della sicurezza nei luoghi di lavoro prevede la possibilità per il datore di lavoro di adottare modelli di organizzazione e di gestione aziendale che consentano di dare effettivo adempimento agli obblighi a tutela dei lavoratori in tale settore (d.lgs. 9 aprile 2008, n. 81, artt. 2 e 30: sul punto si vedano, ad es., linee guida Uni-Inail per un sistema di gestione della salute e sicurezza sul lavoro (sgsl) del 28 settembre 2001 e British *Standard* OHSAS 18001:2007). Nel prendere atto inoltre che il personale universitario, indicato nella richiesta di autorizzazione e nello schema di convenzione fornito dall'ateneo, è da considerarsi, ai fini dell'applicazione della disciplina di settore, ricompreso nella definizione di "lavoratore" di cui all'art. 2, comma 1, lett. *a*), d.lgs. n. 81/2008 e che il quadro normativo applicabile in ordine alla progressiva integrazione fra Ssn ed Università (art. 6, l. 30 novembre 1998, n. 419 e d.lgs. 21 dicembre 1999, n. 517, nonché legge Regione Toscana 24 febbraio 2005, n. 40) attribuisce specifiche funzioni alle "aziende ospedaliere-universitarie", come definite dall'art. 2, d.lgs. n. 517/1999, il Garante ha ritenuto sussistenti i presupposti per autorizzare la comunicazione dei soli dati pertinenti e non eccedenti in vista delle dichiarate finalità (art. 11, comma 1, lett. *d*), del Codice). Posto infine che nell'ambito della tipologia di informazioni destinate alla comunicazione erano state indicate quelle relative allo stato di "maternità" delle lavoratrici, il Garante ha infine precisato che, ai fini dell'applicazione della disciplina di protezione dei dati personali, va considerato dato relativo allo stato di salute (art. 4, comma 1, lett. *d*), del Codice) l'informazione relativa all'interdizione dal lavoro delle lavoratrici in stato di gravidanza ai sensi dell'art. 17 comma 2, lett. *a*), d.lgs. n. 151/2001 (ossia in ragione delle "gravi complicanze della gravidanza o [a] persistenti forme morbose che si presume possano essere aggravate dallo stato di gravidanza"), fattispecie in relazione alla quale i competenti uffici della Direzione Provinciale del Lavoro e della Asl dispongono l'interdi-

zione dal lavoro delle lavoratrici in stato di gravidanza fino al periodo di astensione c.d. obbligatoria (provv. 27 giugno 2013, n. 315, doc. web n. 2576686). Pertanto, ove nell'adempimento di specifici obblighi in capo alle amministrazioni interessate si renda necessario provvedere alla comunicazioni anche di siffatte informazioni ovvero di altri dati sensibili (art. 4, comma 1, lett. *d*), del Codice) – come di già chiarito con provv. 31 luglio 2014 –, si potrà provvedere, se del caso, ad eventuali aggiornamenti dei rispettivi regolamenti per il trattamento dei dati sensibili e giudiziari previo parere del Garante (provv. 2 ottobre 2014, n. 435, doc. web n. 3593920).

13.5. *Il trattamento di dati giudiziari di personale dipendente di società appaltante*

Per quanto riguarda il trattamento di dati giudiziari nell'ambito del rapporto di lavoro, il Garante ha autorizzato una società che svolge attività di pubblico servizio nel settore postale a trattare (nelle forme previste dalla normativa vigente, ovvero l'accesso al casellario giudiziario, ove consentito, o l'autocertificazione degli interessati) informazioni riferite al personale incaricato della effettuazione di servizi postali in virtù di un contratto di appalto di servizi. Considerato che la normativa vigente richiede, per coloro che svolgono attività connesse alla fornitura di servizi postali (ritenuta di preminente interesse generale), l'insussistenza di determinate condizioni personali – condanna a pena detentiva per delitto non colposo superiore a sei mesi o sottoposizione a misure di sicurezza o prevenzione – il fornitore del servizio potrà trattare esclusivamente i dati giudiziari relativi a tale requisito soggettivo (provv. 27 marzo 2014, n. 155, doc. web n. 3117758).

14 Le attività economiche

14.1. *Il settore bancario*

Numerose sono le segnalazioni e i reclami relativi al trattamento dei dati degli interessati da parte delle banche, riguardanti, in particolare, la comunicazione a terzi di informazioni dei clienti, in assenza del preventivo consenso degli stessi e in mancanza di uno dei suoi equipollenti (artt. 23 e 24 del Codice), nonché casi concernenti il trattamento dei dati della clientela effettuati dalle banche senza fornire ai singoli interessati l'informativa di cui all'art. 13 del Codice.

La prima tipologia di casi rappresenta sicuramente una "patologia" del sistema connessa alla particolare "appetibilità" di queste informazioni, soprattutto in alcune situazioni di inevitabile frizione tra le parti (controversie economiche legate a separazioni personali, vicende di carattere successorio, complesse situazioni connesse allo svolgimento delle procedure concorsuali).

In particolare, con provvedimento adottato il 9 gennaio 2014, n. 14 (doc. web n. 2938867), il Garante ha dichiarato l'illiceità del trattamento posto in essere da una finanziaria che ha comunicato a terzi (nel caso di specie il coniuge della reclamante) informazioni relative ad un contratto di finanziamento stipulato dalla stessa con la società. Quest'ultima aveva dichiarato di avere agito in buona fede, avendo fatto affidamento sul fatto che il coniuge della segnalante era stato presente sia durante la fase precontrattuale, sia al momento della sottoscrizione del contratto. Il Garante con il citato provvedimento ha però sostenuto che il titolare del trattamento è sempre tenuto a verificare con scrupolo se il rapporto giuridico che lo lega all'interessato lo legittimi a porre in essere operazioni di trattamento nei confronti di altri soggetti "senza violare gli obblighi nascenti dalla legge o da un rapporto contrattuale". Nel caso di specie detto principio non è stato rispettato. Infatti, il rapporto contrattuale riguardava esclusivamente la reclamante e, quindi, non autorizzava l'accoglimento della richiesta avanzata dal terzo volta a ricevere la documentazione, in quanto lo stesso era estraneo al descritto rapporto.

Analogamente, in un altro provvedimento adottato il 12 novembre 2014, n. 516 (doc. web n. 3657964) il Garante ha dichiarato l'illiceità del trattamento posto in essere dalla banca, che aveva comunicato a terzi informazioni riferite alla reclamante attraverso una lettera inviata oltre che alla stessa reclamante anche ad altri destinatari. Anche in questo caso la banca, nel confermare l'avvenuto invio, aveva dichiarato di ritenere che quanto avvenuto non configurasse una comunicazione di dati a terzi in considerazione di una stretta connessione giuridico-economica tra l'interessata e gli altri soggetti a cui la nota era stata inviata. Con il citato provvedimento, il Garante ha affermato che, nella fattispecie considerata, non rilevavano i legami economici e parentali (pur esistenti in via di fatto) tra i destinatari della comunicazione, che è pertanto avvenuta in assenza del consenso dell'interessata nonché di una delle ipotesi di esonero dello stesso (artt. 23 e 24 del Codice), configurando, in tal modo, un trattamento dei dati personali dell'interessata in violazione anche del principio di liceità e correttezza del trattamento (art. 11, comma 1, lett. *a*), del Codice).

Facendo applicazione dei medesimi principi, in data 25 settembre 2014 il Garante aveva già adottato il provvedimento n. 428 (doc. web n. 3565196) nei confronti di

un'altra banca, dichiarando l'illiceità del trattamento dei dati personali dell'interessata avvenuto attraverso una comunicazione a terzi di informazioni riguardanti un conto corrente bancario alla medesima intestato e ritenendo anche in questo caso che non avesse rilievo il fatto che il terzo destinatario della comunicazione fosse fideiussore di un diverso rapporto bancario riferito all'interessata (segnatamente, di un mutuo ipotecario).

Con riguardo, inoltre, al rispetto dei principi di trasparenza e correttezza che dovrebbero improntare, in generale, il rapporto banca-clientela, il Garante ha ribadito, con provvedimento adottato il 2 ottobre 2014, n. 436 (doc. web n. 3634921), che le banche, in qualità di titolari del trattamento, sono tenute a fornire ai singoli interessati l'informativa di cui all'art. 13 del Codice in vista dell'instaurazione e della gestione del rapporto contrattuale, comprendente anche gli ulteriori, specifici elementi indicati dall'art. 5 del codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di credito al consumo, affidabilità e puntualità nei pagamenti (provv. 16 novembre 2004, n. 8, in *G.U.* 23 dicembre 2004, n. 300, come modificato dall'*errata corrige* in *G.U.* 9 marzo 2005, n. 56 All. A.5. del Codice, doc. web n. 1556693), al fine di evidenziare le particolari modalità di trattamento di tali dati da parte delle cd. centrali rischi private.

Tracciamento delle operazioni bancarie

In considerazione della frequenza e della rilevanza dei casi di illecita comunicazione a terzi di dati ed informazioni bancarie, segnalati e spesso riscontrati dall'Autorità, il Garante, già in data 12 maggio 2011, aveva approvato il provvedimento a carattere generale rivolto all'intero settore creditizio recante "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie" (provv. n. 192, doc. web n. 1813953). Attesa la complessità e l'onerosità degli adempimenti previsti a carico degli istituti di credito, il provvedimento prevedeva però un termine di 30 mesi per la loro implementazione, decorrente dalla data di pubblicazione sulla Gazzetta Ufficiale (avvenuta il 3 giugno 2011, n. 127). Alla luce delle difficoltà tecniche, finanziarie e organizzative rappresentate dagli operatori del settore, tale termine è stato prorogato due volte, da ultimo con provvedimento 22 maggio 2014, n. 257 (doc. web n. 3192807), che ha indicato la data del 30 settembre 2014 come termine finale per il completamento degli adempimenti previsti. Ad oggi, quindi, il provvedimento può finalmente costituire un deterrente nei confronti delle prassi fraudolente, che sono state peraltro alla base della sua adozione. Nei prossimi mesi l'Autorità non mancherà di effettuare accertamenti al fine di verificare in concreto il pieno adempimento della decisione e di raccogliere spunti ed indicazioni operative per meglio monitorare un ambito di trattamento che coinvolge fortemente il rapporto banca-clientela.

Infine, a seguito di apposite richieste di verifica preliminare, l'Autorità ha adottato due provvedimenti in data 6 febbraio 2014, nn. 55 e 56 (doc. web nn. 2986091 e 3000045), relativi all'adozione di impianti di rilevazione delle impronte digitali per l'accesso dei clienti alle proprie cassette di sicurezza, con i quali, nel ribadire la liceità della finalità perseguita dalle banche e la proporzionalità di tale trattamento, ha prescritto le specifiche misure a garanzia degli interessati già indicate nei precedenti provvedimenti adottati in tale ambito negli anni 2012 (provv. 13 settembre 2012, n. 242, doc. web n. 1927441 e provv. 18 ottobre 2012, n. 298, doc. web n. 2212554; cfr. Relazione 2012, p. 199) e 2013 (provv. 14 febbraio 2013, n. 66, doc. web n. 2375735; provv. 19 settembre 2013, n. 406, doc. web n. 2710934).

14.2. *La revisione del codice deontologico Sic*

Il "Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti", che trova applicazione dal 1° gennaio 2005, è uno strumento di fondamentale importanza nel settore creditizio, che ha offerto una cornice regolatoria al fenomeno della cd. referenziazione creditizia, fino alla sua introduzione priva di qualsiasi disciplina. Nonostante il giudizio sostanzialmente positivo sul codice, era già da tempo fortemente avvertita l'esigenza di una sua revisione, prevista, peraltro, dall'art. 13, comma 10 dello stesso codice. Ciò non solo sul piano dell'interpretazione (non sempre univoca di alcune specifiche disposizioni) e dell'applicazione di alcuni principi in esso contenuti, ma anche al fine di tenere conto di problematiche sorte successivamente alla sua sottoscrizione, determinate, soprattutto, da normative ad esso sopravvenute. Anche gli operatori del settore (gestori dei Sic, banche e società finanziarie) si erano già espressi a favore della necessità di un riesame del codice deontologico, da ultimo in occasione dell'attività ispettiva svolta nel 2013 ai sensi dell'art. 13, comma 8, del codice stesso. Pertanto, con provvedimento del 17 aprile 2014, n. 203 (doc. web n. 3070048), il Garante ha invitato gli operatori di settore e gli altri soggetti interessati a partecipare ai lavori di revisione del codice deontologico, stabilendo i criteri per verificare il rispetto del principio di rappresentatività di cui all'art. 2, comma 2, del reg. n. 2/2006 del Garante sulle procedure per la sottoscrizione dei codici di deontologia e di buona condotta. All'esito della consultazione, tenuto conto delle richieste di partecipazione – pervenute sia dai soggetti che già avevano sottoscritto il codice deontologico il 26 ottobre 2004, sia da nuovi soggetti, di cui è necessario valutare attentamente l'effettiva rappresentatività –, l'Autorità ha avviato l'attività di vaglio delle richieste pervenute, il cui completamento è previsto per gli inizi del 2015.

14.3. *La banca dati dei clienti morosi nell'ambito dei servizi di comunicazione elettronica*

Il Garante ha adottato, a seguito di una richiesta pervenuta da Assotelecomunicazioni (Asstel), uno schema di provvedimento volto a definire le condizioni di legittimità per la costituzione di una banca dati finalizzata alla verifica dell'affidabilità e della puntualità nei pagamenti da parte dei clienti nel settore dei servizi di comunicazione elettronica (cd. Sit) (provv. 27 marzo 2014 n. 154, doc. web n. 3041680). Tale banca dati consentirebbe agli operatori del settore tlc di ottenere ulteriori informazioni volte a verificare l'affidabilità dei potenziali clienti, oltre quelle che gli stessi operatori già ricavano dalle banche dati interne ad ogni società, dalle fonti pubbliche, nonché dalla possibilità, recentemente riconosciuta dal legislatore, di accedere ai Sistemi di informazione creditizie (art. 6-*bis*, l. 14 settembre 2011, n. 148). Considerato che il provvedimento va a regolare aspetti che coinvolgono delicati interessi degli utenti dei servizi di comunicazione elettronica, si è ritenuto opportuno avviare una consultazione pubblica sullo stesso, rivolta soprattutto alle associazioni dei consumatori, al fine di acquisirne il contributo. Alla fine del 2014, considerate le numerose osservazioni pervenute, tali da evidenziare posizioni del tutto contrastanti tra gli operatori di settore e le associazioni dei consumatori, l'Autorità ha ritenuto indispensabile avviare un'ulteriore fase di confronto diretto tra le parti, tuttora in corso, al fine di arrivare, se possibile, ad una decisione in grado di contemperare le contrapposte esigenze.

14.4. *Il settore assicurativo*

Il Garante ha esaminato numerose segnalazioni in ambito assicurativo confermando i principi già enunciati in passato. In particolare, alcuni segnalanti hanno contestato la ricezione di comunicazioni aventi ad oggetto solleciti di pagamento di premi assicurativi asseritamente non dovuti, nonostante l'opposizione all'ulteriore trattamento di dati previamente manifestata in occasione dell'invio di comunicazioni di recesso tempestivamente presentate. In tali casi, a seguito di specifica attività istruttoria, l'Autorità, ribadendo i principi di liceità e correttezza enunciati dall'art. 11 del Codice, ha ritenuto illecito, limitatamente al profilo in questione, il trattamento effettuato dalle società di assicurazioni nei confronti degli interessati con la conseguente impossibilità di utilizzare i relativi dati personali.

14.5. *La videosorveglianza in ambito privato*

Come attestato dalle numerose segnalazioni, nonché dalle diverse istanze di verifica preliminare, la videosorveglianza resta tra gli ambiti più seguiti dall'opinione pubblica.

Per ciò che concerne in particolare le segnalazioni e i reclami, si può osservare che, oltre alle tematiche più consuete, riguardanti comunicazioni relative ad impianti di videosorveglianza istallati in asserita violazione dei principi sanciti dal Codice ed in particolare del provvedimento di carattere generale sulla videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680), sono emersi nuovi profili relativi all'utilizzo delle telecamere per nuove esigenze (controllo di minori negli asili, finalità di ricostruzione di sinistri a scopi assicurativi, etc.) anche attraverso l'uso di nuove apparecchiature di ripresa messe a disposizione dall'evoluzione tecnologica (ad es., i droni dotati di videocamere e le cd. *dashcam*).

Di qui la necessità di predisporre un aggiornamento del citato provvedimento generale in materia di videosorveglianza del 2010, attività che sarà completata presumibilmente nel corso del presente anno anche tenendo anche conto della recente sentenza della CGUE (11 dicembre 2014, causa C-212/13, František Ryneš c. Ú ad pro ochranu osobních údaj, doc. web n. 3845146). Quest'ultima, nel fornire un'interpretazione autentica della nozione di "esercizio di attività a carattere esclusivamente personale o domestico" in relazione all'utilizzo da parte di una persona fisica di videocamere installate in corrispondenza della propria abitazione per proteggere i beni, la salute e la vita dei proprietari della medesima e tale tuttavia da sorvegliare anche lo spazio pubblico prospiciente, con registrazione continua delle immagini riprese, influenzerà le future determinazioni dell'Autorità, specie in merito all'individuazione delle ipotesi rientranti nella clausola di esclusione dal novero del trattamento di dati personali di cui all'art. 5, comma 3, del Codice.

Per ciò che riguarda, invece, le istanze di verifica preliminare, vale rilevare che tutte hanno riguardato la richiesta di allungare i tempi di conservazione delle immagini registrate dai sistemi di videosorveglianza oltre i sette giorni (previsti in termini generali dal citato provvedimento del 2010) al fine di rafforzare sostanzialmente gli *standard* di sicurezza di determinati ambiti produttivi.

In genere, si è trattato di imprese che operano nel campo della produzione di strumenti di precisione o nei settori della logistica e dei trasporti intermodali di merci (ivi compresa l'effettuazione di tutte quelle attività che riguardano le importazioni ed esportazioni dei prodotti e le relative pratiche doganali). Tutte le richieste hanno avuto un esito favorevole da parte del Garante (v. provv.ti 30 gennaio 2014, n. 40,

doc. web n. 3017416; 13 marzo 2014, n. 121, doc. web n. 3117736 e 18 settembre 2014, n. 409, doc. web n. 3457674), il quale le ha valutate tenendo in considerazione non solamente i parametri di sicurezza previsti dalle normative internazionali, comunitarie e nazionali, soprattutto in materia doganale e nel settore dell'aviazione civile, ma valorizzando anche i requisiti previsti da alcuni sistemi di certificazione volontaria che, benché non vincolanti, sono comunemente considerati nei settori di riferimento come *standard* per garantire al meglio, ad esempio, la sicurezza nella fornitura di prodotti o nella prestazione di servizi ad alto contenuto tecnologico, nonché la migliore gestione dei centri logistici e delle merci ivi custodite.

14.6. *Il recupero crediti*

Un numero elevato di segnalazioni pervenute in materia di recupero stragiudiziale dei crediti ha evidenziato la persistenza di condotte che, a seguito dell'attività istruttoria avviata dall'Autorità, non si sono rivelate conformi al provvedimento generale adottato dal Garante il 30 novembre 2005 (doc. web n. 1213644).

A fronte di una segnalazione concernente solleciti di pagamento preregistrati inviati da una banca, l'Ufficio ha ritenuto che il sistema utilizzato non garantisse l'accertamento dell'identità di colui che rispondeva alla chiamata poiché si limitava a rimettere all'interlocutore la mera facoltà di confermare di essere il titolare del finanziamento, mediante l'inserimento delle ultime due cifre dell'anno di nascita.

In altri casi, talune società di recupero crediti sono stata invitate a rimodulare la locuzione contenuta nell'intestazione della corrispondenza utilizzata per i solleciti di pagamento poiché considerata suscettibile di palesare l'informazione relativa all'asserito stato di inadempimento del destinatario della comunicazione.

Sempre nell'ambito di tale attività, viste le risultanze istruttorie, il Garante ha adottato il provvedimento 20 marzo 2014, n. 136 (doc. web n. 3115085) nel quale ha riaffermato il principio, già sancito nel 2005, secondo cui chiunque effettui un trattamento di dati personali nell'ambito di una attività di recupero crediti, in ossequio ai principi di liceità e correttezza (art. 11, comma 1, lett. *a*), del Codice), deve astenersi dal "comunicare ingiustificatamente a soggetti terzi rispetto al debitore (quali ad es., familiari, coabitanti, colleghi di lavoro o vicini di casa) informazioni relative alla condizione di inadempimento nella quale versa l'interessato", avendo cura di evitare "nel tentativo di prendere contatto con il medesimo (anche attraverso terzi) comportamenti suscettibili di incidere sulla sua dignità". La società titolare del trattamento in esame, infatti, nel tentativo di contattare il segnalante, anche presso il proprio posto di lavoro, aveva riferito al suo superiore gerarchico la situazione di insolvenza in cui si trovava l'interessato, perpetrando, ovviamente, un trattamento illecito, in contrasto sia con le regole generali del Codice (artt. 2, 11 e 23) sia con le previsioni specifiche del richiamato provvedimento generale del 2005.

14.7. *La propaganda elettorale.*

Successivamente all'adozione del provvedimento generale in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale (v. par. 4.5), l'Autorità è intervenuta nei confronti di una casa di cura che aveva utilizzato i dati personali di un *ex*-assistito (ormai defunto), acquisiti in occasione di un pregresso ricovero, per inviare comunicazioni dall'innegabile contenuto propagandistico-elettorale (provv. 31 luglio 2014, n. 393, doc. web n. 3407167).

L'Autorità ha ritenuto che lo specifico trattamento di dati personali effettuato dalla casa di cura nel caso in esame fosse illecito, perché svolto in assenza di idonei presupposti giustificativi (informativa e consenso dell'interessato, al tempo non acquisito) e in violazione del principio di finalità (artt. 11, comma 1, lett. *b*), 13 e 23 del Codice), che impone di utilizzare i dati personali in operazioni di trattamento compatibili con gli scopi sottesi alla loro raccolta. Il Garante ha quindi vietato alla società l'ulteriore trattamento di tali dati per l'invio di nuove comunicazioni di analogo tenore (artt. 143, comma 1, lett. *c*), 144 e 154, comma 1, lett. *d*), del Codice), prescrivendo al contempo alla stessa di astenersi, in futuro, dall'utilizzare ingiustificatamente, e per le medesime finalità, i dati personali degli altri assistiti detenuti per scopi diversi dalla propaganda elettorale.

15 I dati biometrici

15.1. *La casistica*

Considerato il crescente interesse per l'utilizzo di sistemi di rilevazione biometrica, l'Autorità ha continuato ad esaminare numerose richieste di verifica preliminare aventi ad oggetto il trattamento di tale peculiare tipologia di dati, in particolare acquisiti attraverso l'analisi delle caratteristiche dinamiche della firma autografa apposta dagli utenti su dispositivi *hardware* impiegati in ambito bancario. Ferme restando le ipotesi di esonero da ultimo previste nell'apposito provvedimento generale adottato dal Garante in materia (cfr. par. 15.2) e le correlate dichiarazioni di conformità rese dai titolari sulla base delle prescrizioni ivi formulate, l'Autorità si è pronunciata su un distinto caso relativo all'utilizzo di dati biometrici a fini di autenticazione nelle procedure di sottoscrizione con firma digitale di documenti e modulistica bancaria. Conformandosi all'orientamento già espresso negli anni precedenti (v. Relazione 2012, p. 206 e ss.), l'Autorità ha ribadito, con provvedimento 23 gennaio 2014, n. 25 (doc. web n. 2938921), che il trattamento dei dati biometrici di natura comportamentale connesso all'utilizzo di sistemi complessi qual è quello di firma digitale remota con autenticazione biometrica, può ritenersi lecito solo se effettuato con il libero consenso degli interessati e previo rilascio a questi ultimi di un'informativa adeguata ed esaustiva. Inoltre, devono essere sempre rispettati, oltre ai principi di liceità e finalità del trattamento (art. 11, comma 1, lett. *a*) e *b*), del Codice), quelli di necessità e proporzionalità (artt. 3 e 11, comma 1, lett. *d*), del Codice), avuto anche riguardo alle modalità di configurazione del sistema (che, nel caso esaminato, avrebbero consentito il trattamento dei dati biometrici degli interessati in forma "disgiunta" dai relativi dati anagrafici, sì da permetterne l'identificazione solo indirettamente). Il Garante, nel valutare positivamente il sistema sottoposto alla sua attenzione, ha tuttavia prescritto ai co-titolari del trattamento ulteriori misure e accorgimenti a protezione dei dati biometrici dei firmatari, in particolare attraverso l'adozione di presidi tecnico-organizzativi in grado di ridurre i rischi di alterazione dei dispositivi e di installazione di *software* o applicazioni potenzialmente pericolosi. Infine, sono stati stabiliti, in conformità alle disposizioni di legge (art. 11, comma 1, lett. *e*), del Codice), i tempi di conservazione dei dati degli interessati, rapportandoli alle finalità e alle funzionalità del servizio.

Per altro verso, l'Autorità è stata chiamata a valutare un distinto trattamento di dati biometrici basato sui rilievi dattiloscopici degli interessati per finalità di accesso ai *caveaux* di una società operante nel settore della conservazione e custodia di beni, merci e oggetti di rilevante valore economico, nonché della contazione e selezione di banconote e monete metalliche per conto terzi (provv. 17 aprile 2014, n. 205, doc. web n. 3239985). Muovendo da alcune precedenti pronunce, il Garante ha ritenuto proporzionato il trattamento oggetto dell'istanza, sia alla luce della delicatezza delle attività svolte dalla società (meritevoli, già di per sé, di elevati *standard* di affidabilità e sicurezza), sia in ragione delle specifiche finalità perseguite e del peculiare contesto in cui la stessa ha dichiarato di operare (tale da giustificare, nella prospettiva indicata, un accertamento particolarmente rigoroso degli utenti in ingresso ai *caveaux*). L'Autorità, nel prendere atto che le modalità del trattamento indicate

non risultavano in violazione dei principi di necessità e proporzionalità, ha ricordato come il consenso al trattamento possa ritenersi effettivamente libero solo se sia realmente assicurata agli interessati la possibilità di fruire di modalità alternative di accesso ai *caveaux* (artt. 11, comma 1, lett. *a*) e 23 del Codice); la società, che aveva già fornito rassicurazioni in tal senso, è stata comunque invitata ad integrare l'informativa resa agli interessati, con specifico riferimento all'utilizzo della tecnologia Rfid applicata alle *smartcard* adoperate dagli utenti. È stato infine precisato che i dati trattati, accessibili unicamente da incaricati del trattamento autorizzati e adeguatamente istruiti, potranno essere conservati dalla società anche oltre i tempi stabiliti, ma solo in presenza di eventi criminosi o di richieste provenienti dall'autorità giudiziaria o dagli stessi interessati.

15.2. *Il provvedimento generale sul trattamento dei dati biometrici*

A seguito delle plurime decisioni assunte dall'Autorità nel corso degli anni (e delle quali si è dato conto nelle precedenti relazioni annuali), il Garante ha adottato, tenuto conto degli esiti della consultazione pubblica svoltasi tra il 23 maggio e il 22 giugno 2014, il provvedimento generale in tema di biometria 12 novembre 2014, n. 513 (doc. web n. 3556992). Grazie ad esso si intende consentire ai titolari di trattamento di evitare l'interpello del Garante per la verifica preliminare ai sensi dell'art. 17 del Codice, purché i trattamenti di dati biometrici risultino compresi entro il perimetro di semplificazione individuato dal provvedimento medesimo, tenuto conto delle finalità del trattamento (in particolare in relazione a forme di autenticazione informatica, per il controllo di accesso fisico ad aree "sensibili" e utilizzo di apparati e macchinari pericolosi, per la sottoscrizione di documenti informatici nonché per scopi cd. facilitativi) e del tipo di caratteristica biometrica prescelta, e vengano adottate le misure di sicurezza previste a protezione dei dati personali biometrici nonché garantite, ove richiesto dal Garante, modalità alternative di perseguimento delle finalità del trattamento che non implichino il ricorso a dati biometrici. Le finalità ammesse e le caratteristiche biometriche previste per usufruire dell'esonero sono sintetizzate nella seguente tabella.

FINALITÀ	CARATTERISTICHE BIOMETRICHE AMMESSE
Autenticazione informatica	Impronte digitali, voce
Controllo di accesso fisico ad aree "sensibili" e utilizzo di apparati e macchinari pericolosi	Impronte digitali, topografia della mano
Scopi facilitativi	Impronte digitali, topografia della mano
Sottoscrizione di documenti informatici con firma elettronica avanzata	Firma autografa

Con il provvedimento il Garante ha inoltre adottato le Linee guida (che ne fanno parte integrante) in materia di riconoscimento biometrico e firma grafometrica (doc. web n. 3563006), con cui vengono fornite informazioni ai titolari del trattamento, ai produttori di tecnologie biometriche, ai fornitori di servizi e agli

interessati sui diversi aspetti connessi alla protezione dei dati personali, ivi compresi quelli relativi alla sicurezza nonché sui presupposti di legittimità dei trattamenti dei dati biometrici. Si è così stabilito che, con particolare riguardo ai casi di:

- autenticazione informatica, le caratteristiche biometriche dell'impronta digitale o dell'emissione vocale di una persona possono essere utilizzate come credenziali di autenticazione per l'accesso a banche dati e sistemi informatici. Tale trattamento può essere effettuato anche senza il consenso dell'utente;
- controllo di accesso fisico ad aree "sensibili" e utilizzo di apparati e macchinari pericolosi, le caratteristiche dell'impronta digitale o della topografia della mano potranno essere trattate per consentire l'accesso ad aree e locali ritenuti "sensibili" oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati. Tale trattamento può essere realizzato anche senza il consenso dell'utente;
- sottoscrizione di documenti informatici, l'analisi dei dati biometrici associati all'apposizione a mano libera di una firma autografa potrà essere utilizzata per la firma elettronica avanzata. Questa modalità è però consentita solo con il consenso degli interessati, consenso non necessario invece in ambito pubblico, se devono essere perseguite specifiche finalità istituzionali. Dovranno comunque essere resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici;
- utilizzo per scopi cd. facilitativi, l'impronta digitale e la topografia della mano potranno essere utilizzate anche per consentire l'accesso fisico di utenti ad aree fisiche in ambito pubblico (es. biblioteche) o privato (es. aree aeroportuali riservate). Anche in questo caso l'utilizzo è consentito solo con il consenso degli interessati. Dovranno comunque essere previste modalità alternative per l'erogazione del servizio per chi rifiuta di far utilizzare i propri dati biometrici.

Ogni sistema di rilevazione dovrà essere configurato in modo tale da raccogliere un numero limitato di informazioni (principio di minimizzazione) e previa adozione delle numerose misure di sicurezza individuate dal Garante (ad es., quella che obbliga a cifrare il riferimento biometrico con tecniche crittografiche, con una lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati). Anche al fine di prevenire eventuali furti di identità biometrica, tutte le violazioni dei dati o gli incidenti informatici (*data breach*) che possano avere un impatto significativo sui sistemi biometrici o sui dati personali custoditi, dovranno essere comunicati da chi detiene i dati al Garante entro 24 ore dalla scoperta, così da consentire di adottare opportuni interventi a tutela delle persone interessate. A tal fine è stato predisposto un modulo che consente di semplificare il predetto adempimento. Sono esclusi dalle modalità semplificate individuate nel provvedimento del Garante i trattamenti che prevedono la realizzazione di archivi biometrici centralizzati, per i quali continuerà ad essere obbligatorio richiedere una verifica preliminare. Rimane in vigore anche l'obbligo di notificazione al Garante per i trattamenti non esplicitamente esclusi dal provvedimento, come quelli effettuati da esercenti le professioni sanitarie e da avvocati.

16 Il trattamento dei dati nel condominio

A seguito dell'entrata in vigore, nel giugno del 2013, della legge 11 dicembre 2012, n. 220, recante modifiche alla disciplina del condominio negli edifici, cittadini e associazioni di categoria hanno sottoposto all'Autorità diversi quesiti circa l'esatta interpretazione di alcune delle nuove norme ivi contenute; ciò con particolare riferimento alle disposizioni di cui agli artt. 1129, comma 7, c.c. in ordine alla previsione di un conto corrente intestato al condominio e all'art. 1130, comma 1, punto 6, c.c. relativo all'obbligo di tenuta da parte dell'amministratore del cd. registro di anagrafe condominiale.

Al riguardo, il Garante ha chiarito che il condomino non è tenuto a fornire alcuna prova documentale delle informazioni rese all'amministratore per la costituzione del predetto registro di anagrafe condominiale; su altro fronte, può invece chiedere all'amministratore copia integrale, senza oscuramenti, degli atti e dei documenti bancari relativi al conto corrente intestato al condominio.

In ordine al primo aspetto, l'Autorità ha ribadito che l'amministratore può trattare solo informazioni pertinenti e non eccedenti rispetto alle finalità da perseguire. Al fine di adempiere correttamente al nuovo obbligo sancito dalla riforma, l'amministratore può, quindi, legittimamente acquisire le informazioni che consentono di identificare e contattare i singoli partecipanti al condominio – siano essi proprietari, usufruttuari, conduttori o comodatari delle unità immobiliari – richiedendo, come stabilito dalla norma, le cd. generalità, comprensive del codice fiscale, della residenza o del domicilio. Può chiedere, inoltre, le informazioni volte ad individuare catastalmente le singole unità immobiliari (cd. estremi di identificazione catastale), ossia: la sezione urbana, il foglio, la particella, il subalterno e il comune. Per quanto concerne poi le informazioni relative alle condizioni di sicurezza, con l'entrata in vigore del cd. decreto destinazione Italia (d.l. 23 dicembre 2013, n. 145), i condòmini non dovranno più fornire alcuna informazione sulla propria unità immobiliare, perché i dati da raccogliere riguardano ora solo le parti comuni dell'edificio.

A riprova della veridicità delle informazioni rese, il condomino non è però tenuto, perché risulterebbe eccedente, ad allegare alcuna eventuale ulteriore documentazione (ad es., l'atto di compravendita in cui sono riportati i dati).

Con riferimento alla novità introdotta dal legislatore nell'art. 1130 c.c., l'Autorità ha evidenziato (nota 31 marzo 2014) che, a seguito della riforma, deve essere aperto e utilizzato dall'amministratore un conto condominiale, al quale ciascun condomino, seppur per il tramite dello stesso amministratore, può accedere. In particolare, il Garante ha chiarito che nonostante il conto sia intestato alla compagine condominiale nella sua complessità, i singoli condòmini sono titolari di una posizione giuridica che consente loro di verificare la destinazione dei propri esborsi e l'operato dell'amministratore mediante l'accesso in forma integrale ai relativi estratti conto bancari o postali. Tale principio, già sancito in linea generale dal Garante nelle Linee guida in ambito bancario (provv. 25 ottobre 2007, doc. web n. 1457247), comporta infatti il diritto di ottenere "copia di atti o documenti bancari" senza alcuna limitazione, neanche nelle forme di un parziale oscuramento, anche se contengono dati personali di terzi. Nel confermare l'attualità dei principi già stabiliti da questa Autorità in passato in materia di trattamento di dati personali e di amministrazione

di condomini con il provvedimento generale del 18 maggio 2006 (doc. web n. 1297626), si è colta l'occasione anche per ribadire che resta fermo in capo alla stessa compagine condominiale (nella qualità di titolare del trattamento) – di regola per il tramite dell'amministratore (nell'eventuale veste di responsabile del trattamento) –, l'obbligo di adottare le idonee misure di sicurezza atte a prevenire illecite comunicazioni e diffusioni di dati personali raccolti anche ai fini della tenuta del predetto registro, tutto ciò ai sensi e per gli effetti degli artt. 31 e ss. del Codice (cfr. provv. 18 maggio 2006, punto 3.3).

Nell'ambito delle istruttorie aperte dall'Autorità, il Garante è stato inoltre chiamato (provv. 19 giugno 2014, n. 314, doc. web n. 3275910 e provv. 30 ottobre 2014, n. 482, doc. web n. 3658161) a definire alcune controversie inerenti il tema della divulgazione dei dati personali nell'ambito delle attività connesse all'amministrazione dei condomìni. Ciò con specifico riferimento al trattamento di dati personali effettuato da amministratori che hanno inviato solleciti di pagamento o comunque attestazioni di uno stato di morosità dell'inquilino a terzi (in un caso al datore di lavoro mediante l'invio ad un indirizzo *e-mail* accessibile da chiunque sul posto di lavoro, in un altro ad un'agenzia di intermediazione immobiliare coinvolta nella vendita di un immobile sito nel relativo condominio), anziché allo stesso inquilino personalmente. L'Autorità, in ambedue i casi, è intervenuta accertando l'avvenuto trattamento di dati in modo non conforme alla legge. Il Garante ha altresì prescritto agli amministratori coinvolti in dette vicende di adottare le misure necessarie in grado di assicurare effettivamente il rispetto delle regole poste dal Codice a tutela della comunicazione di dati personali a terzi e di impartire adeguate istruzioni in merito al personale in servizio presso gli studi ove gli stessi operano.

17 Le libere professioni

17.1. *L'attività forense e investigativa*

Trattamento dei dati da parte di investigatori privati

Nel valutare una segnalazione, l'Autorità ha chiarito gli ambiti di legittimità delle investigazioni private finalizzate ad acquisire elementi di prova nell'ambito delle controversie civili per quanto riguarda l'obbligo di fornire all'interessato l'informativa di cui all'art. 13 del Codice (nota 19 maggio 2014). Nella specie, l'attività investigativa era volta ad acquisire elementi relativi alla capacità economica dell'interessato, di professione medico, ed era stata commissionata dalla moglie in relazione ad una causa di separazione giudiziale. Un collaboratore dell'investigatore, per comprovare il maggior reddito dell'interessato rispetto alle risultanze della documentazione fiscale, si era recato in incognito – ossia, senza fornire alcuna informativa in merito all'attività investigativa in corso – presso lo studio del medico, con il pretesto di sottoporsi ad una visita clinica, a seguito della quale riportava l'informazione che il medico non aveva rilasciato la ricevuta fiscale; il collaboratore effettuava altresì, clandestinamente, riprese fotografiche del professionista al fine della sua sicura identificazione.

Il titolare dell'agenzia investigativa aveva giustificato la mancata informativa all'interessato invocando l'art. 13, comma 5, lett. *b*), del Codice, in quanto i dati del segnalante erano trattati esclusivamente per far valere o difendere un diritto in sede giudiziaria, per il periodo strettamente necessario a tal fine. L'Autorità, invece, ha ritenuto illegittimo il trattamento in argomento, in quanto l'esenzione dall'obbligo di fornire l'informativa, prevista dal citato art. 13, comma 5, del Codice, opera solo con riferimento "alla disposizione di cui al comma 4" del medesimo articolo, relativa al caso in cui "i dati personali non sono raccolti presso l'interessato", mentre nel caso in esame i dati erano stati acquisiti direttamente presso l'interessato. Del resto, l'autorizzazione n. 6/2013 relativa al trattamento dei dati sensibili da parte degli investigatori privati (doc. web n. 2819019) testualmente prescrive che "l'interessato o la persona presso la quale sono raccolti i dati deve essere informata ai sensi dell'art. 13 del Codice, ponendo in particolare evidenza l'identità e la qualità professionale dell'investigatore, nonché la natura facoltativa del conferimento dei dati. Nel caso in cui i dati siano raccolti presso terzi, è necessario informare l'interessato e acquisire il suo consenso scritto (art. 13, commi 1, 4 e 5 e art. 26, comma 4, del Codice), solo se i dati sono trattati per un periodo superiore a quello strettamente necessario per esercitare il diritto in sede giudiziaria o per svolgere le investigazioni difensive [...]. Tale orientamento, espresso già in passato (provv. 19 febbraio 2002, doc. web n. 1063652), è condiviso anche dalla giurisprudenza (Trib. Bergamo, 31 luglio 2002, n. 4436 e Cass., 15 luglio 2005, n. 15076).

Uso del fax

Con riferimento all'uso, da parte di un avvocato, del fax per l'invio – nel caso di specie ritenuto di per sé legittimo – ad una società di comunicazioni contenenti dati personali di un dipendente della medesima, l'Autorità ha ricordato (nota 22 settembre 2014) che l'utilizzo del fax per comunicazioni giudiziarie è ben noto al vigente codice di procedura civile. In particolare, il Giudice può autorizzare il difensore a provvedere alle notificazioni degli atti giudiziari attraverso mezzi particolari (art. 151 c.p.c.), tra i quali è compreso il fax (cfr. Cass., Sez. lav., 21 luglio

2008, n. 20078); inoltre, l'art. 250 c.p.c. (come modificato dall'art. 2, comma 3, d.l. 14 marzo 2005, n. 35, convertito con modificazioni dalla l. 14 maggio 2005, n. 80) stabilisce che l'intimazione a comparire ai testimoni ammessi dal giudice istruttore può essere effettuata dal difensore attraverso l'invio di copia dell'atto mediante lettera raccomandata con avviso di ricevimento, a mezzo di telefax, oppure di posta elettronica, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici e teletrasmessi. Inoltre, nel caso in esame, il Giudice aveva formalmente autorizzato la parte a procedere alla comunicazione degli atti, anziché alla notificazione. Né è valso a rendere illegittimo l'uso del *fax* la circostanza che tale mezzo di comunicazione, ove usato per trasmettere documenti ad organizzazioni complesse come una società, può determinare l'apprensione dei dati ivi contenuti da parte di persone non abilitate ad accedervi. Infatti, proprio in considerazione della necessità di assicurare la tutela della riservatezza dei dati personali anche nell'ambito delle strutture complesse, il Codice prescrive al titolare del trattamento di designare per iscritto gli incaricati del trattamento, i quali – e solo essi – possono effettuare le operazioni di trattamento dei dati, sotto l'autorità del titolare (o del responsabile), attenendosi alle istruzioni prescritte (art. 30 del Codice). Inoltre, il titolare del trattamento è tenuto ad adottare tutte le misure di sicurezza necessarie ad assicurare il corretto trattamento dei dati personali (art. 33 del Codice). Pertanto, è obbligo della società adottare le misure organizzative che assicurino che la conoscenza dei dati personali sia possibile solo per coloro che sono incaricati del loro trattamento. Peraltro, ferma la legittimità dell'invio della comunicazione a mezzo fax, l'Autorità ha richiamato l'attenzione delle parti a considerare l'opportunità, nel caso di eventuali ulteriori comunicazioni di tale natura, di utilizzare canali di comunicazione (quale la corrispondenza in busta chiusa) che consentano una maggiore tutela della riservatezza dei soggetti i cui dati personali sono contenuti nella documentazione trasmessa, anche tenendo conto delle particolari cautele introdotte dal Codice in materia di notifica di atti giudiziari.

Obbligo di informativa del cliente da parte dell'avvocato

In ordine all'obbligo di informativa che l'avvocato deve rendere al proprio cliente ai sensi dell'art. 13 del Codice, è stato sottoposto al Garante un caso in cui il legale, antecedentemente al primo appuntamento presso il suo studio, aveva acconsentito a ricevere via *e-mail* documentazione contenente dati personali, anche giudiziari, da un potenziale cliente. A seguito del mancato conferimento dell'incarico al legale ed alla richiesta di questo del compenso professionale per l'attività svolta sulla documentazione inviata, l'interessato lamentava di non avere ricevuto dall'avvocato l'informativa relativa al trattamento dei suoi dati personali. L'Autorità ha ritenuto illegittimo il trattamento dei dati personali effettuato dal professionista, in quanto l'informativa di cui all'art. 13 del Codice deve essere fornita all'interessato prima del trattamento dei suoi dati. È pur vero che prima dell'incontro presso lo studio legale i contatti tra le parti erano avvenuti solo attraverso posta elettronica e che fu l'interessato a proporre all'avvocato la trasmissione dei documenti contenenti i suoi dati giudiziari affinché quest'ultimo potesse valutarli ed esprimere "un parere con cognizione di causa" nel successivo incontro. Tuttavia, l'avvocato consentì espressamente, tramite *e-mail* inviata all'interessato, a tale trasmissione ed a trattare successivamente i dati ivi contenuti senza fornire all'interessato l'informativa dovuta. Ove il professionista avesse voluto ispirare la sua condotta al rispetto della disciplina sulla tutela dei dati personali, avrebbe dovuto previamente fornire all'interessato l'informativa di cui all'art. 13 del Codice, ad esempio con la *e-mail* con la quale acconsentiva a ricevere dal segnalante i suoi dati personali (nota 16 aprile 2014).

Registrazione video e telefonica da parte di un avvocato degli incontri avvenuti con la clientela

Un avvocato ha posto un quesito sulla possibilità di effettuare riprese degli incontri avuti con i clienti e di registrare le conversazioni telefoniche con essi intercorse, adducendo esigenze di natura probatoria nell'ipotesi di contestazioni relative all'espletamento del mandato e, in generale, di sicurezza e tutela del patrimonio e dei professionisti operanti nello studio. L'Ufficio ha richiamato le disposizioni più rilevanti del contesto normativo disciplinante la fattispecie in esame, precisando che deve aversi riguardo, quale criterio fondamentale per considerare i singoli casi dubbi, al principio generale di proporzionalità nel trattamento di dati, nel senso di pertinenza e non eccedenza dei dati ai sensi dell'art. 11 del Codice. In proposito, si è rilevato che tale principio induce a dubitare che la astratta eventualità di situazioni pregiudizievoli, esemplificate in termini del tutto generali ovvero con mero riferimento a fatti di cronaca, possa di per sé dimostrare che nel singolo caso ricorrono circostanze che giustificano le modalità del trattamento oggetto del quesito (nota 19 settembre 2014).

Altre segnalazioni

Pervengono frequentemente segnalazioni che ritengono non conformi al Codice condotte tenute da avvocati nei confronti dei propri clienti. Tuttavia l'Autorità ha rilevato che molti dei comportamenti segnalati non attengono alla disciplina dei dati personali (come nel caso del mancato deposito da parte di un avvocato dell'atto di rinuncia all'incarico professionale nel fascicolo di ufficio relativo alla controversia, ai sensi dell'art. 85 c.p.c., o in quello della mancata restituzione della documentazione ricevuta dalla parte assistita per l'espletamento del mandato, che è regolata dall'art. 42 del Codice deontologico forense), sì che la valutazione di detti comportamenti non rientra tra i compiti istituzionali dell'Autorità (cfr. note 15 ottobre e 7 novembre 2014).

18 Il trasferimento dei dati all'estero

La materia dei trasferimenti transfrontalieri di dati personali è stata oggetto di costante attenzione da parte del Garante sia in occasione dell'attiva partecipazione dell'Autorità ai lavori del Gruppo Art. 29, sia con riferimento, a livello nazionale, alle numerose istanze volte al rilascio di autorizzazioni al trasferimento di dati verso Paesi terzi tramite le cd. *Binding corporate rules* (Bcr).

Anche nel corso dell'anno di riferimento è stato confermato il crescente interesse da parte del settore privato (in particolare, delle società di carattere multinazionale) all'utilizzo delle Bcr quale strumento per il trasferimento infragruppo di dati personali (per lo più di quelli relativi ai clienti, dipendenti e fornitori delle società facenti parte del gruppo richiedente) verso Paesi terzi. Il numero di richieste di autorizzazione giunte è stato elevato e il relativo *iter* si è concluso con l'approvazione di nove autorizzazioni rilasciate dal Garante al termine di complesse istruttorie, ove è stata verificata la conformità del testo delle Bcr, approvato al termine delle procedure europee di mutuo riconoscimento, con l'ordinamento italiano e con alcuni dei principali criteri stabiliti in materia dal Gruppo Art. 29 (cfr., fra gli altri, provv. 23 gennaio 2014, n. 27, doc. web n. 3058168; provv. 15 maggio 2014, n. 246, doc. web n. 3233476; provv. 26 giugno 2014, n. 325, doc. web n. 3320773; provv. 9 ottobre 2014, n. 449, doc. web n. 3635086). Ma il 2014 si è caratterizzato soprattutto per l'esame da parte dell'Autorità di alcune Bcr consistenti, a differenza dei casi affrontati negli anni precedenti (ove erano generalmente previste soluzioni contrattuali: cfr. Relazione 2013, p. 123), esclusivamente da dichiarazioni unilaterali sottoscritte dalle società capogruppo o, in taluni casi, in semplici regole di condotta (cd. *privacy policy*). Trattandosi di fattispecie che presentano profili di più incerta qualificazione nell'ordinamento giuridico nazionale, il Garante, al fine di rilasciare le relative autorizzazioni, ha ritenuto opportuno effettuare maggiori approfondimenti oltre a quelli di regola condotti nell'ambito delle precedenti istruttorie. A tal fine l'Autorità ha preso in considerazione e reputato rilevanti specifici aspetti volti ad accertare la cd. "vincolatività interna" (ossia la garanzia dell'effettivo rispetto delle Bcr da parte dei membri del gruppo e del personale dipendente: cfr. WP 74, par. 3.3.1) concernenti: l'impegno della capogruppo e delle altre società del gruppo ad osservare i principi contenuti nelle Bcr stesse (ivi comprese le clausole di responsabilità e del terzo beneficiario); l'avvenuta approvazione delle Bcr ad opera del consiglio di amministrazione della capogruppo, da cui discende l'obbligo di osservanza delle stesse da parte di tutte le società e del personale dipendente del gruppo; la sussistenza del potere della capogruppo, in virtù della propria posizione di controllo, di richiedere alle altre società l'attuazione delle Bcr; la previsione, in caso di mancata osservanza delle Bcr, di un sistema di sanzioni disciplinari nei confronti del personale dipendente; la realizzazione all'interno delle società di un programma di controllo volto ad assicurare il raggiungimento degli obiettivi aziendali tra cui il rispetto delle politiche in materia di protezione dei dati.

Una volta accertati tali aspetti in sede di istruttoria, l'attenzione è stata poi rivolta all'ulteriore profilo della cd. vincolatività esterna (ossia la garanzia per l'interessato di veder soddisfatti i diritti a lui riconosciuti all'interno delle Bcr: cfr. in merito WP 74, par. 3.3.2). Al riguardo, nei relativi provvedimenti di autorizzazione (provv. 4 dicem-

bre 2014, nn. 560 e 561, doc. web nn. 3668394 e 3668436) è stato evidenziato come l'art. 44, comma 1, lett. *a*), del Codice – a seguito della modifica apportata al testo, anche in ragione della presentazione al Parlamento e al Governo di una specifica segnalazione in materia (cfr. segnalazione 8 novembre 2007, doc. web n. 1467485) –, riconosce ora espressamente il potere del Garante di autorizzare un trasferimento di dati personali verso Paesi terzi anche nel caso in cui tale trasferimento sia posto in essere tramite regole di condotta esistenti nell'ambito di società appartenenti ad un medesimo gruppo, purché le stesse presentino adeguate garanzie per i diritti dell'interessato. È stato pertanto ritenuto che in virtù di tale previsione normativa, le predette regole di condotta possano costituire un fatto idoneo a produrre effetti giuridicamente vincolanti nell'ordinamento nazionale, ai sensi dell'art. 1173 c.c.

Alla luce di tali valutazioni, l'Autorità ha reso alle società istanti le relative autorizzazioni, ribadendo al contempo che l'interessato, in base al diritto nazionale applicabile, può, in ogni caso, far valere i propri diritti nel territorio dello Stato anche in ordine all'inosservanza delle garanzie contenute nelle Bcr (art. 44, comma 1, lett. *a*), del Codice) e che il Garante, in virtù dei poteri attribuitigli dal Codice, ai sensi degli artt. 154 e 157, può svolgere in qualsiasi momento i necessari controlli sulla liceità e correttezza del trasferimento dei dati e, comunque, su ogni operazione di trattamento ad essi inerente, nonché adottare, se necessario, i provvedimenti previsti dalla normativa nazionale applicabile.

19 Il registro dei trattamenti

19.1. *La notificazione*

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

Le notificazioni sono inserite in un registro pubblico liberamente e gratuitamente consultabile *online* tramite il sito dell'Autorità, da cui chiunque può acquisire notizie e utilizzarle per le finalità di applicazione della disciplina in materia di protezione dei dati personali (ad es., per esercitare il diritto di accesso ai dati o gli altri diritti riconosciuti dal Codice).

È importante tenere sempre in considerazione che la notificazione del trattamento deve essere presentata al Garante prima dell'inizio del trattamento, una sola volta, indipendentemente dal numero delle operazioni e dalla durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate. Una nuova notificazione è richiesta solo prima che cessi definitivamente l'attività di trattamento oppure quando si renda necessario modificare alcuno degli elementi in essa contenuti.

Sui titolari che hanno notificato un trattamento incombe l'onere di mantenere aggiornato il registro comunicando le eventuali variazioni (ad es. il cambio di sede o la denominazione della società) o la cessazione del trattamento (ad es., in occasione della cessazione dell'impresa). Nel caso in cui una pluralità di soggetti autonomi esercitano congiuntamente un potere decisionale sulle finalità e sulle modalità di un trattamento di dati personali in modo tale che si realizzi una vera e propria "contitolarità", ciascuno di essi è tenuto ad effettuare un'autonoma notificazione, nella quale indicherà anche gli altri contitolari.

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

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

19.2. *Il registro dei trattamenti a dieci anni dalla sua istituzione*

Nel 2014 il nuovo registro dei trattamenti, istituito con il Codice a decorrere dal 1° gennaio 2004, ha compiuto dieci anni: può quindi risultare interessante

verificare, al di là delle delle notificazioni effettuate nel 2014 (cfr. sez. IV, tab. 17), come sia cambiata la mappa dei trattamenti notificati al Garante.

Nel 2004 sono state effettuate n. 10.014 notificazioni al registro dei trattamenti, con la compilazione di n. 15.084 tabelle relative ai vari tipi di trattamento (una singola notificazione, ovviamente, può riguardare più tipologie di trattamento). Alla fine del 2014 erano invece presenti sul registro dei trattamenti n. 24.075 notificazioni, con n. 35.488 tabelle compilate (cfr. sez. IV, tab. 14).

Le varie tipologie di trattamenti notificati hanno avuto un andamento piuttosto variabile nel corso di questi dieci anni, come si può verificare dai dati analitici inerenti l'evoluzione su base annua delle varie tabelle compilate dai titolari del trattamento (cfr. sez. IV, tab. 12 e 13 e grafico 15).

Volendo però fotografare in maniera sintetica l'attuale distribuzione delle tipologie di trattamento presenti sul registro delle notificazioni alla fine del 2014, effettuando una comparazione con la situazione verificatasi all'avvio del nuovo registro nell'anno 2004 (cfr. sez. IV, tab. 16), è possibile osservare in particolare che:

- la notificazione di trattamenti di dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 37, comma 1, lett. *b*) ha registrato una riduzione dell'incidenza percentuale sul totale dei trattamenti, passando dal 24,3% del 2004 al 21,1% del 2014;
- la notificazione di trattamenti relativi alle "banche dati sulla solvibilità e le frodi" (art. 37, comma 1, lett. *f*) si è ridotta, passando da un'incidenza relativa del 21% nel 2004 al 18,5% del 2014;
- parallelamente, in questo decennio è aumentata in percentuale la notificazione di trattamenti relativi alla cd. "geolocalizzazione" (art. 37, comma 1, lett. *a*), passati da una percentuale del 7,7% nel 2004 al 9,9% nel 2014 e, soprattutto, si è registrata una crescita consistente nella notificazione dei trattamenti inerenti la cd. "profilazione" (art. 37, comma 1, lett. *d*), incrementatisi dal 23,7% del 2004 al 28,9% del 2014.
- per gli altri trattamenti di cui all'art. 37, l'incidenza relativa sul totale delle notificazioni non ha subito grossi scostamenti a tutto il 2014 rispetto alla situazione rilevata nell'anno 2004.

Sotto il profilo della natura pubblica o privata del titolare del trattamento, è possibile riscontrare che dal 2004 al 2014 è aumentata l'incidenza dei soggetti privati che hanno notificato trattamenti, rispetto ai soggetti pubblici. Infatti, dall'88% di titolari del trattamento privati che avevano notificato almeno una tipologia di trattamento alla fine del 2004, si è passati, alla fine dell'anno 2014, ad una percentuale del 91%, con un corrispondente decremento nella percentuale di soggetti pubblici (cfr. sez. IV, grafico 18).

Sotto un altro profilo, appare interessante notare, come peraltro prevedibile, che esistono alcune rilevanti differenze nelle tipologie di trattamenti notificate a seconda della natura pubblica o privata del titolare (cfr. sez. IV, grafico 19). Alla fine del 2014, infatti, la principale categoria di trattamenti notificata da titolari aventi natura pubblica ha riguardato i dati di cui all'art. 37, comma 1 lett. *b*), del Codice ("dati idonei a rivelare lo stato di salute e la vita sessuale [...]") – riepilogati nella tab. 4 del registro dei trattamenti – con una percentuale del 28% sul totale dei trattamenti notificati da soggetti pubblici al 31 dicembre 2014. Al secondo posto troviamo il trattamento di dati genetici (art. 37, comma 1, lett. *a*), del Codice – tab. 1 reg. trattamenti), con una percentuale del 17% circa e, al terzo posto, il trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (art. 37, comma 1 lett. *a*), del Codice – tab. 3 reg. trattamenti), con una percentuale del 15%.

Per i soggetti privati, alla stessa data di rilevazione, la principale tipologia di trattamento notificata è risultata essere quella relativa alla cd. "profilazione" (art. 37, comma 1, lett. *d*), del Codice), con una percentuale del 31% circa, mentre i trattamenti di dati di cui alla tab. 4 del registro si classificano solo in seconda posizione con una percentuale del 20% sul totale, seguiti a loro volta dai trattamenti di dati relativi alle cd. "banche dati sulla solvibilità e le frodi" (art. 37, comma 1, lett. *f*), del Codice – tab. 8 reg. trattamenti), che rappresentano il 19% del totale.

In generale possiamo dire che l'adempimento "notificazione" così come reinterpretato nel 2003 dal Codice (limitato cioè solo ad alcune tipologie di trattamento) è un adempimento che ha avuto un certo impatto e una discreta diffusione.

Già nel 2005, il Gruppo Art. 29, nell'ambito di una propria riflessione sull'istituto della notificazione, aveva osservato che la notificazione conservava una particolare valenza soprattutto nei Paesi di recente adesione all'UE, laddove rivestiva una funzione general-preventiva di richiamo dell'attenzione sull'esistenza di particolari obblighi connessi alla legislazione sulla protezione dei dati (cfr. Relazione sull'obbligo di notifica da parte delle autorità di controllo nazionali, sull'utilizzo più appropriato di eccezioni e semplificazioni e sul ruolo degli incaricati per la protezione dei dati in ambito UE 18 gennaio 2005 - WP 106). In contesti nei quali, invece, la disciplina di protezione dei dati personali è più matura, tra i quali possiamo sicuramente annoverare l'Italia, esso invece tende ad essere considerato come un mero adempimento burocratico. Nella società odierna, in cui la dinamicità del trattamento dei dati passa attraverso semplici interazioni degli utenti con *app* e dispositivi interconnessi (*Internet of things*), la staticità della notificazione appare sempre più inadeguata a garantire efficacemente i diritti degli interessati.

In questo senso, quindi, nella proposta di nuova regolamentazione europea in corso di approvazione si supererà la logica della notificazione a vantaggio di nuovi strumenti più effettivi, primo fra tutti l'introduzione della nuova figura del *data protection officer* (definito nella traduzione italiana, in maniera un po' infelice, "Responsabile della protezione dei dati") – i cui compiti sono ancora in corso di definizione –, "presidio avanzato" presso il titolare del trattamento del rispetto dei principi e degli adempimenti in materia nonché interlocutore ed elemento di connessione tra il titolare del trattamento e l'Autorità.

19.3. *L'attività di supporto per i titolari del trattamento e di controllo sul registro*

Il Garante fornisce quotidianamente supporto a tutti i soggetti che notificano i trattamenti sul registro per agevolare la corretta conclusione delle procedure e chiarire eventuali dubbi sui trattamenti che necessitano di essere notificati.

Nel 2014 è proseguita anche un'assidua attività di controllo, sia nei confronti dei titolari iscritti nel registro sia nei confronti di quelli che effettuano trattamenti oggetto di notificazione ma che non risultano presenti nel registro, effettuata anche mediante ispezioni *in loco* (v. al riguardo quanto riportato al par. 22).

In particolare, dalle verifiche effettuate sono emersi 16 casi di omessa/ritardata notificazione del trattamento con riferimento, rispettivamente a: trattamenti di dati biometrici (5); trattamenti di dati genetici (3); trattamenti di dati idonei a rivelare lo stato di salute (4); trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (3); trattamenti di dati con finalità di profilazione.

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

20 La trattazione dei ricorsi

20.1. *I profili generali*

Racchiudendo in uno sguardo d'insieme l'esperienza pluriennale, nell'ambito dell'attività decisionale su ricorsi può dirsi essersi consolidata una "giurisprudenza" dell'Autorità che, in particolare su alcuni "filoni", costituisce ormai un sicuro riferimento, ben conosciuto da tutti i soggetti interessati e largamente sostenuto anche dai giudici aditi in sede di opposizione ai sensi dell'art. 152 del Codice.

Ciò spiega perché alcune tematiche, oggetto di ampio contenzioso in passato, occupino ormai uno spazio marginale. Basti pensare alle richieste di accesso ai dati personali di tipo valutativo, con particolare riguardo a quelli contenuti nelle perizie medico legali redatte in ambito assicurativo; il tema, oggetto di numerosi ricorsi negli anni precedenti, ha trovato oggi un suo assestamento, sia in relazione alle situazioni nelle quali la richiesta di accesso a tali dati è accolta (e quindi rapidamente soddisfatta), sia in riferimento ai pochi casi nei quali tale accesso è differito in ragione della presenza di legittime esigenze difensive e di tutela delle ragioni del titolare del trattamento (art. 8, comma 2, lett. *e*), del Codice). La valutazione della sussistenza di un effettivo pregiudizio deve essere fatta in concreto dal Garante, sulla base degli elementi forniti dal titolare del trattamento o comunque desumibili dagli atti, come avvenuto nel caso di un'azienda sanitaria che ha legittimamente invocato il differimento del diritto di accesso adducendo ragioni volte a non pregiudicare l'esercizio del proprio diritto di difesa nella fase precontenziosa che, in ragione delle iniziative già intraprese dall'interessata, risultava preludere all'instaurazione di una controversia giudiziaria (cfr. provv. 3 luglio 2014, n. 346, doc. web n. 3347884).

Se si guarda al numero complessivo di ricorsi pervenuti all'Autorità e all'insieme dei temi affrontati, si può parlare senz'altro di "incremento" e di "evoluzione" del carico di lavoro. In particolare, dall'esame del numero delle decisioni adottate (306) si evince che si tratta di un numero rilevante di procedimenti, che ha subito un notevole incremento (pari al 38%) rispetto all'anno precedente (222), mentre le tipologie principali dei procedimenti instaurati corrispondono grosso modo ad ambiti già familiari all'Autorità.

20.2. *Dati statistici*

Per ciò che concerne la tipologia delle decisioni, si conferma l'alto numero di decisioni di non luogo a provvedere (60% del totale), cioè di procedimenti conclusisi con il soddisfacimento, nel corso dell'istruttoria, delle richieste degli interessati/ricorrenti. Una percentuale così alta di procedimenti conclusisi velocemente e positivamente depone a favore dell'utilità e dell'efficacia di questa specifica forma di tutela, la cui funzione principale è quella di favorire la composizione delle controversie direttamente tra l'interessato e il titolare del trattamento; tale obiettivo viene perseguito assicurando, da un lato, che i diritti tutelati dall'art. 7 del Codice siano esercitati con richieste mirate e chiare e, dall'altro, che il riscontro del titolare sia tempestivo e pertinente. Sul piano della tipologia delle decisioni va poi sottolineato un andamento costante per ciò che concerne i casi di accoglimento (totale o par-

ziale) delle richieste dei ricorrenti (9%). Costante è anche la percentuale delle decisioni dichiarate infondate (15%) o inammissibili (16%), categoria quest'ultima in cui rientrano anche i provvedimenti adottati per mancata regolarizzazione ai sensi dell'art. 148, comma 2, del Codice (cfr. sez. IV, tab. 4).

Non meno significativo è lo sguardo alle principali categorie di titolari del trattamento, sia pubblici che privati, tra i quali si caratterizzano alcune macro-categorie: in primo luogo banche e società finanziarie, a seguire gli operatori nel settore del *marketing*, i gestori di sistemi di informazioni creditizie come pure di altri archivi centralizzati relativi alla verifica della affidabilità delle imprese, i fornitori di servizi telefonici e telematici nonché le amministrazioni condominiali (cfr. sez. IV, tab. 5). A sottolineare l'attuale momento storico, sono i numerosi ricorsi concernenti il trattamento dati legato all'attività economica; va altresì rilevato il numero significativo di procedimenti attivati nei confronti dei datori di lavoro pubblici e privati. Tale dato riflette le difficoltà occupazionali e la crisi che sta attraversando il mondo del lavoro ed evidenzia il profilo del "nuovo" contenzioso rispetto all'utilizzo delle moderne tecnologie sul luogo di lavoro. Un aspetto di rilevante interesse in questo ambito è la necessità di garantire, in un'ottica di bilanciamento tra i contrapposti interessi, la tutela del diritto del dipendente alla segretezza delle proprie comunicazioni. Considerata infatti l'equivalenza tra la corrispondenza tradizionale e quella elettronica, occorre assicurare un elevato livello di tutela anche alle comunicazioni scambiate dal dipendente con soggetti esterni o interni alla struttura aziendale, tenuto conto del fatto che l'eventuale trattamento di tali dati implicherebbe un'operazione idonea a rendere conoscibili talune informazioni personali relative all'interessato. La necessità di tutela, particolarmente evidente laddove l'*account* di posta elettronica aziendale assegnato in dotazione al dipendente sia individualizzato, ovvero contenga il nome e cognome del medesimo, implica che l'eventuale trattamento dei dati riferiti a comunicazioni di posta elettronica inviate e ricevute dal dipendente presso il menzionato *account* sia tale da evitare un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori. Questa considerazione vale anche nell'ipotesi in cui, per qualunque causa, venga a cessare il rapporto di lavoro o di collaborazione tra le parti rendendo di fatto non più legittimamente utilizzabile dal datore di lavoro, né per inviare la posta in uscita né per ricevere quella in entrata, un *account* di posta elettronica aziendale riconducibile ad un soggetto che non fa più parte dell'organizzazione; tale circostanza rende altresì necessaria l'adozione di misure idonee ad informare i terzi estranei della disattivazione dell'indirizzo medesimo, con contestuale indicazione di un diverso indirizzo di posta elettronica aziendale cui inviare le comunicazioni attinenti la sfera lavorativa (cfr. provv. 27 novembre 2014, n. 551, doc. web n. 3718714).

Significativa anche la decisione del 17 luglio 2014, n. 370 (doc. web n. 3405174) con cui il Garante ha parzialmente accolto il ricorso di un alto dirigente di una società che, sospeso in via cautelare dal servizio per la ritenuta commissione di un grave illecito, era stato privato degli strumenti aziendali in dotazione (*pc, I-phone* e *I-pad*) con relativa disattivazione delle schede Sim e dell'*account* di posta elettronica al fine di effettuare verifiche e accertamenti sul corretto utilizzo degli stessi. Al riguardo, l'Autorità, pur ritenendo lecita l'attività di controllo svolta dalla società (che peraltro ha dichiarato che i controlli avrebbero riguardato esclusivamente l'indirizzo di posta elettronica aziendale), si è pronunciata favorevolmente nei confronti dell'istanza del ricorrente di poter accedere ai propri dati personali contenuti nella corrispondenza elettronica intrattenuta tramite il proprio *account* aziendale (salvo il differimento ai sensi dell'art. 8, comma 2, lett. *e*), del Codice, invocato dalla società resistente per i soli dati acquisiti nel corso delle verifiche esperite sull'*account* del ricorrente); ciò considerato che l'indirizzo di posta elettronica aziendale utilizzato

dal ricorrente era un indirizzo individualizzato recante nome e cognome dello stesso – e non un indirizzo condiviso tra più lavoratori – tale quindi da dover essere considerato dato personale, anche a prescindere dal contenuto della corrispondenza.

Ma la novità che emerge dalla comparazione dei dati con l'anno precedente è l'incremento (dal 10 al 14%) del numero dei ricorsi nei confronti degli editori, anche televisivi (in merito v. *infra* par. 20.3).

Si evidenziano, infine, casi ancora frequenti di ricorsi che vengono proposti da società commerciali ed enti vari, forse ignari del fatto che, a seguito delle modifiche normative intervenute alla fine del 2011 con riguardo alle nozioni di "interessato" e di "dato personale" (art. 4 del Codice), i soggetti diversi dalle persone fisiche sono stati privati della possibilità di utilizzare gli strumenti di tutela previsti dal Codice, qui con particolare riguardo all'esercizio del diritto d'accesso.

20.3. *La casistica più significativa*

Se, come accennato, abitualmente i ricorsi si incentrano su materie ormai note all'Autorità – si pensi all'ambito lavorativo, all'opposizione a trattamenti svolti per finalità promozionali, all'accesso a informazioni bancarie e finanziarie (anche per ricostruire posizioni contabili relative a persone defunte), ovvero alle istanze di cancellazione di posizioni "negative" da alcuni grandi archivi pubblici e privati (centrale dei rischi di Banca d'Italia, Archivio CAI, Sistemi di informazioni creditizie) –, merita qui soffermarsi su alcune decisioni adottate dal Garante con riguardo al trattamento dei dati per finalità giornalistiche, con un'attenzione speciale ai trattamenti svolti tramite i cd. archivi storici *online* dei principali quotidiani nonché ai trattamenti effettuati da parte dei motori di ricerca cd. generalisti.

Trattamenti in ambito giornalistico

Sta assumendo ormai una particolare rilevanza il filone delle richieste di deindicizzazione dai motori di ricerca cui si affiancano da ultimo le richieste di aggiornamento dei dati rivolte agli editori titolari degli archivi *online*. Questa ultima categoria di procedimenti, oggetto peraltro di recente intervento da parte della Corte di giustizia nel caso *Google Spain* (sulla quale v. il par. 23.3), conferma come attraverso lo strumento dei ricorsi pervengano all'attenzione dell'Autorità richieste di intervento sui temi più attuali.

La necessità di ricercare soluzioni tecniche idonee a garantire l'effettivo esercizio del diritto di rettifica e di aggiornamento delle notizie diffuse in rete è emersa da una pronuncia della Corte di Cassazione (n. 5525 del 5 aprile 2012) che ha espressamente riconosciuto il diritto all'aggiornamento e all'integrazione delle notizie lesive per l'interessato ove superate dagli eventi (come nel caso del soggetto noto alla cronaca giudiziaria per essere stato indagato ma di cui si taccia poi del tutto l'avvenuto proscioglimento o, in caso di condanna, l'intervenuta riabilitazione). Il richiamo agli sviluppi successivi rispetto alla notizia originaria consente, da un lato, di tutelare la dignità del soggetto leso e, dall'altro, di migliorare la stessa qualità dell'informazione, che risulta in tal modo esatta ed aggiornata.

Nel prevedere l'obbligo per il titolare di un archivio *online* di contestualizzare nel tempo le informazioni, la sentenza richiamata ha affermato che le necessarie integrazioni per aggiornare la notizia debbano avvenire "con modalità tecniche non modificative dell'originale", rimettendo in capo ai titolari la scelta in merito alle corrette modalità di attuazione.

Sul tema dell'aggiornamento delle notizie è utile analizzare l'orientamento interpretativo nel tempo assunto dal Garante: inizialmente, le richieste volte ad ottenere l'aggiornamento di notizie giudiziarie – specie se non indicizzate dai motori di

ricerca – non venivano accolte in quanto si ritenevano interventi modificativi del contenuto originario degli articoli che, nati come espressione di libera manifestazione del pensiero, venivano poi legittimamente conservati per finalità di documentazione all'interno di archivi. Questi ultimi, benché informatizzati, assolvendo la medesima funzione storica degli archivi cartacei, ben potevano pertanto contenere gli articoli pubblicati secondo il loro contenuto originario.

Con tali decisioni rese dall'Autorità, la tutela riconosciuta all'interessato consisteva nel non rendere più indicizzabili, dai motori di ricerca esterni al sito in cui l'archivio è contenuto, le sole pagine web contenenti gli articoli oggetto di contestazione. Le informazioni – anche se non aggiornate – restavano comunque reperibili direttamente nell'archivio storico del giornale.

In seguito alla menzionata sentenza della Corte di Cassazione n. 5525/2012, l'Autorità ha invece espressamente riconosciuto il diritto "ad ottenere l'aggiornamento/integrazione dei dati personali che lo riguardano quando eventi e sviluppi successivi (adeguatamente documentati) hanno modificato le situazioni oggetto di cronaca giornalistica (seppure a suo tempo corretta) incidendo significativamente sul profilo e l'immagine dell'interessato". Si è così prescritto all'editore titolare del trattamento, non solo di deindicizzare gli articoli non aggiornati, ma anche, e soprattutto, di predisporre nell'ambito dell'archivio storico *online* del quotidiano, un sistema idoneo a segnalare (ad es., a margine dei singoli articoli o in nota agli stessi) la sopravvenienza di nuovi elementi ed il loro contenuto (come nel caso di intervenuta definizione in via giudiziaria della vicenda) consentendone il rapido ed agevole accesso al lettore. Così la decisione di accoglimento parziale del ricorso contro una testata giornalistica nazionale a cui il Garante ha ordinato di predisporre, nell'ambito dell'archivio storico *online* del relativo quotidiano, un sistema di aggiornamento/integrazione degli articoli in questione idoneo a fornire ai lettori l'immediata visibilità degli sviluppi informativi facendo sì che gli stessi emergessero già nell'anteprima dell'articolo presente tra i risultati del motore di ricerca dell'archivio storico (provv. 9 gennaio 2014, n. 9, doc. web n. 3001832).

Un ulteriore passo in avanti si è registrato con una decisione dell'11 dicembre 2014, n. 604 (doc. web n. 3732971) che ha riconosciuto l'idoneità di una soluzione "tecnica" che rende effettivo l'aggiornamento di una notizia anche quando la stessa continua ad essere reperibile sui motori di ricerca generalisti. Nel caso in esame, il ricorrente aveva chiesto (tra l'altro) l'adozione di un sistema idoneo a segnalare l'esistenza del seguito della notizia in relazione ad un articolo del maggio 2013 – rinvenibile sul web associato al proprio nominativo – pubblicato su un quotidiano locale *online* e riferito ad una vicenda giudiziaria nella quale era stato coinvolto. Ed invero, il procedimento penale avviato nei suoi confronti (avviso di garanzia) e riportato dalla testata *online* si era concluso con l'adozione di un decreto di archiviazione per non aver commesso il fatto. Tale notizia era stata successivamente riportata in un articolo pubblicato nel novembre successivo dalla medesima testata ma della stessa non era fatta alcuna menzione nell'articolo originario.

In particolare, non si contestava la liceità della notizia come originariamente pubblicata (avviso di garanzia) quanto piuttosto la mancanza di un sistema idoneo ad informare il lettore di un seguito della stessa (archiviazione). Il ricorrente precisava inoltre che digitando soltanto il proprio nominativo era possibile rinvenire nel motore di ricerca entrambe le notizie, mentre utilizzando chiavi di ricerca diverse (come ad es., i nomi degli altri soggetti menzionati nell'articolo quali, ad es., altri indagati, l'avvocato o il consulente) i risultati riportavano esclusivamente l'articolo iniziale relativo all'indagine penale avviata (anche) nei suoi confronti. Pertanto, la notizia, originariamente corretta, se non aggiornata, risulta a distanza di tempo parziale e non esatta.

Nel corso dell'istruttoria l'editore resistente ha provveduto non soltanto ad inibire ai motori di ricerca l'accesso all'articolo attraverso la compilazione del *file* "*robots.txt*", ma ha apposto in calce all'articolo originario un *link* nel quale è possibile rinvenire la notizia dell'avvenuta archiviazione del procedimento penale a carico del ricorrente.

L'Autorità ha affrontato nel dicembre 2014, per la prima volta dopo la citata sentenza della Corte di giustizia nel caso Google Spain, le problematiche che coinvolgono ormai direttamente non soltanto gli editori-titolari dei quotidiani *online* ma anche, e soprattutto, i motori di ricerca che, sebbene non qualificabili come editori, sono comunque da considerarsi titolari del trattamento dei dati contenuti nei relativi indici e, in quanto stabiliti sul territorio di uno Stato membro, sono tenuti a rispettare le disposizioni nazionali in materia di protezione dei dati. Nel caso di specie (provv. 18 dicembre 2014, n. 618, doc. web n. 3736353), la richiesta formulata da un ricorrente volta alla deindicizzazione dell'indirizzo url che lo riguardava, rinvenibile attraverso Google, non è stata accolta dal momento che le notizie rinvenibili a tale indirizzo, pubblicate nel giugno 2014, erano assai recenti nonché di pubblico interesse, riguardando un'importante indagine giudiziaria. Nella medesima decisione, tuttavia, l'Autorità ha affrontato un profilo delicato riguardante le modalità con le quali i dati/informazioni riferiti ad un soggetto sono associati e, quindi, visualizzati dagli utenti nel cd. *snippet*. Come noto ogni risultato di ricerca è sostanzialmente composto da un titolo e da una descrizione, un *abstract* che riporta, in breve, le parole chiave utilizzate dall'utente nella stringa di ricerca – e che spesso sono rese più evidenti utilizzando una grafica particolare. Nel caso di specie, il ricorrente lamentava il fatto di aver rivestito una posizione marginale rispetto ai reati di usura ed estorsione menzionati nel titolo dell'articolo indicizzato dal motore di ricerca, mentre l'*abstract* associava espressamente il suo nominativo alle parole "misure cautelari" facendo così presumere – erroneamente – che lo stesso fosse stato sottoposto anche a misure restrittive della libertà personale. Il ricorrente ha pertanto fatto valere la pretesa a che l'*abstract* visualizzato sotto il titolo dell'articolo "non associ genericamente", per mezzo delle scansioni operate automaticamente dal motore di ricerca, il proprio nominativo alle notizie principali dell'articolo (riassunte nel titolo), indipendentemente dalla specifica narrazione dei fatti relativi all'interessato come riferiti. Il motore di ricerca ha provveduto a rimuovere integralmente lo *snippet* associato all'indirizzo *url* contenente l'articolo. L'aspetto più rilevante della decisione richiamata riguarda il fatto che l'Autorità ha ritenuto legittima la richiesta avanzata dal ricorrente affinché anche l'*abstract* visualizzato dalle ricerche effettuate non associ genericamente, per mezzo delle scansioni operate automaticamente dal motore di ricerca, il nominativo dell'interessato alle notizie principali contenute nell'articolo indicizzato e, dunque, indipendentemente dalla specifica narrazione dei fatti.

Appare evidente come il tema in esame, richieda un adeguamento costante, con particolare riferimento alle soluzioni tecniche necessarie a codificare ed implementare i principi giuridici.

21 Il contenzioso giurisdizionale

21.1. *Considerazioni generali*

Come riferito nella Relazione 2013, l'art. 34, d.lgs. n. 150/2011, ha abrogato l'art. 152 del Codice – con l'eccezione del comma 1 – dettando all'art. 10 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 78 ricorsi notificati nel 2012 e dei 32 nel 2013, nel 2014 sono stati notificati al Garante e da questo trattati 31 ricorsi.

Attesa l'utilità 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, assume sempre maggiore rilevanza l'obbligo – purtroppo non sempre puntualmente adempiuto – per le cancellerie di trasmettere al Garante copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal Codice o in materia di criminalità informatica (art. 154, comma 6).

Tale 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 dell'evoluzione della giurisprudenza in materia di protezione dei dati personali e di svolgere il ruolo di segnalazione al Parlamento e al Governo degli interventi normativi necessari per la tutela dei diritti degli interessati (come previsto dall'art. 154, comma 1, lett. *f*), del Codice).

21.2. *I profili procedurali*

In tema di giurisdizione, l'Autorità non ha avuto notizia di ricorsi concernenti il trattamento dei dati personali proposti avanti al giudice amministrativo né di pronunce che hanno dichiarato un difetto di competenza per materia.

21.3. *I profili di merito*

Sono pervenute, in numero minore rispetto agli anni precedenti, decisioni dell'autorità giudiziaria, nell'ambito di giudizi nei quali non erano in discussione provvedimenti adottati dal Garante. Appare al riguardo utile, in quanto attiene alla rilevanza nei rapporti civili della disciplina in materia di protezione dati, soffermarsi sulle pronunce relative a richieste di risarcimento danni.

Tra le più significative, si segnala quella con cui la Corte di Cassazione ha ritenuto che l'invio di una comunicazione concernente l'apertura del procedimento

disciplinare da parte dell'ufficio al quale era assegnato l'interessato, non solo agli uffici periferici di un'amministrazione statale, ma anche alla Direzione centrale, non costituisce violazione della normativa in materia di protezione dei dati, svolgendo la Direzione stessa una funzione di controllo, indirizzo e coordinamento. È stata confermata la sentenza di primo grado, su questo punto, nonché in relazione all'illiceità della comunicazione dell'appartenenza sindacale dell'interessato; è stata invece rilevata l'erroneità della sentenza circa l'inammissibilità della prova per testi al fine di provare un'affezione fisica o psichica subita dal ricorrente. In proposito la Corte ha affermato che, poiché il danno non patrimoniale non può mai ritenersi *in re ipsa* ma va allegato e provato da chi lo invoca, anche attraverso presunzioni semplici, a maggior ragione può essere provato tramite testimoni (Cass., 16 aprile 2013, n. 22100).

In altro caso, la Corte di appello di Trento, sezione distaccata di Bolzano (3 dicembre 2013, n. 174), si è pronunciata sulla richiesta di risarcimento del danno in conseguenza della diffusione su due quotidiani e un sito web delle generalità e di altri dati idonei ad identificare l'interessata, in relazione ad un fatto di cronaca in conseguenza del quale, peraltro, la stessa era deceduta. Il giudice ha confermato che, pur nella singolarità della vicenda, non vi era necessità, per la completezza dell'informazione, di fornire i dati personali e l'immagine della persona deceduta non rivestendo la stessa alcun ruolo pubblico. In ordine alla pretesa risarcitoria fatta valere dalla figlia dell'interessata, è stato affermato che il danno non patrimoniale – suscettibile di prova mediante presunzioni – racchiude ogni ipotesi in cui sia stato leso un valore inerente la persona, non esaurendosi nel danno morale soggettivo, e liquidato in oltre undicimila euro, essendosi ritenuto menomato il diritto alla riservatezza e sussistente la sofferenza psichica dell'interessata per essere stata esposta alla curiosità dei lettori.

In un caso per alcuni aspetti simile – in cui era stata riportata da un quotidiano la notizia di un incidente stradale che vedeva coinvolta una famiglia, della quale sono stati pubblicati dati che consentivano un facile riconoscimento degli interessati – il giudice ha negato la sussistenza del danno non patrimoniale, in quanto ha ritenuto che amici, parenti, conoscenti e anche sconosciuti, che rivestirono di indesiderata attenzione i soggetti interessati raggiungendoli personalmente o telefonicamente nei giorni immediatamente successivi alla pubblicazione del fatto di cronaca, difficilmente non avrebbero avuto altrimenti notizia del grave incidente in un piccolo centro come quello di residenza della famiglia in questione (Trib. Messina, 27 novembre 2014, n. 2392).

Alcune pronunce hanno riguardato la richiesta di risarcimento del danno nei confronti di società operanti nel campo finanziario da parte di privati in relazione a segnalazioni negative a sistemi di intermediazione creditizia.

In due casi il giudice ha ritenuto che non fosse stato provato da parte della resistente l'invio all'interessato del preavviso che deve precedere la segnalazione a sofferenza ai sensi dell'art. 4, comma 7 del codice di deontologia per i sistemi informativi.

Per quanto attiene al danno non patrimoniale, nel primo caso il giudice ha rilevato che a configurare la risonanza negativa, tra gli intermediari del settore creditizio, in ordine all'affidabilità e solvibilità del ricorrente è sufficiente, trattandosi di conseguenze ordinarie, la mera allegazione del fatto illecito (Trib. Roma, 21 novembre 2013, n. 23617).

Nel secondo caso, il giudice ha affermato che, a prescindere dall'attività economica eventualmente esercitata dal danneggiato, l'illegittima segnalazione può determinare, oltre ad un danno patrimoniale, anche una lesione di fondamentali diritti del debitore, quali quello all'immagine ed alla reputazione, con ciò non dovendosi ritenere che si tratti di un danno *in re ipsa*; infatti per la segnalazione in una banca

dati per un tempo sufficiente a consentirne la percepibilità da parte di coloro che hanno ad essa accesso, può ritenersi verificata la presunzione di un danno non patrimoniale (Trib. Milano, 8 maggio 2014, n. 5911).

In entrambi i casi il ristoro del danno è stato determinato in 5.000,00 euro.

Sempre in materia di segnalazione presso centrali rischi, un privato era stato fatto oggetto di alcune segnalazioni a sofferenza, di cui una per un importo molto consistente, la cui erroneità l'istituto bancario resistente aveva riconosciuto doversi ricondurre ad errore tecnico procedurale. Il giudice, riprendendo le argomentazioni suesposte circa la risarcibilità del danno, ha ritenuto, vista l'entità dell'importo e il fatto che la cancellazione del nominativo del ricorrente, nonostante le numerose richieste avanzate dallo stesso, era avvenuta dopo quasi due anni, sussistente il danno non patrimoniale, determinato in 90.000,00 euro (Trib. Milano, 5 marzo 2014, n. 3215).

21.4. *Le opposizioni ai provvedimenti del Garante*

L'anno 2014 ha registrato un lieve incremento nella proposizione delle opposizioni a provvedimenti dell'Autorità: a fronte dei sessantasette ricorsi del 2013, nel 2014 sono state proposte ottanta opposizioni. Di queste, quarantaquattro si riferiscono a opposizioni a ordinanze ingiunzioni (di cui quattro a verbale di contestazione, inammissibili per costante giurisprudenza), con sostanziale stabilità rispetto al 2013, nel quale le impugnazioni di tale natura erano state trentotto.

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

Trentacinque 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 all'anno 2014, si è confermata la tendenza dei giudici a ridurre in alcuni casi l'importo delle sanzioni irrogate dall'Autorità.

Tra le opposizioni alle ordinanze ingiunzioni, tre decisioni hanno riguardato provvedimenti irroganti sanzioni in relazione a trattamenti di immagini raccolte mediante impianti di videosorveglianza, rispettivamente, in quattro esercizi commerciali e nei locali di una impresa individuale. Nell'ultimo caso la decisione ha riguardato anche l'omessa informativa relativa al trattamento dati operato dal sito internet dell'impresa. In tutti i casi le valutazioni dell'Autorità sono state confermate ed i ricorsi rigettati (Trib. Padova, 8 aprile 2014, n. 1155; Trib. Lecce, 6 giugno 2014, n. 2206 e Trib. Venezia, 17 luglio 2014, n. 1596).

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. Roma, 17 settembre 2013, n. 18376)

In tema di *e-mail* promozionali, il Tribunale di Modena (5 giugno 2014, n. 989) 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 al grado di responsabilità accertato e, per quanto concerne la condotta contestata, all'immediata sospensione dell'attività vietata, nonché in considerazione dell'applicazione al caso di specie

della più favorevole l. n. 166/2009, entrata in vigore anteriormente all'emanazione dell'ordinanza ingiunzione.

Il Tribunale di Milano, in analoga fattispecie, ha confermato il provvedimento ingiuntivo, rilevando che la disciplina posta dall'art. 23 del Codice impedisce automatismi tra la mera iscrizione ad un sito internet e la possibilità per il gestore di inviare comunicazioni con contenuto commerciale, poiché i dati dei singoli utenti che prendono parte a gruppi di discussione in internet, come nel caso di specie, non possono essere utilizzati per fini diversi qualora manchi un consenso specifico degli interessati (31 ottobre 2013, n. 13664).

Sempre il Tribunale di Milano ha ridotto l'entità della sanzione irrogata, in un caso di omessa informativa relativamente all'invio di sms ad un *database* di anagrafiche che la società ricorrente aveva ricevuto dalla società proprietaria ed in seguito aveva ceduto ad un terza società senza aver fornito l'informativa agli interessati e senza aver raccolto dagli stessi il relativo consenso. L'organo giudicante ha ritenuto di escludere, in quanto non adeguatamente emersa nell'istruttoria, la sussistenza dell'aggravante *ex* art. 164-*bis* applicata in ragione dell'elevato numero di interessati coinvolti nelle violazioni (5 febbraio 2014, n. 1748).

È stato altresì confermato il provvedimento ingiuntivo a carico di una persona che aveva inviato una *e-mail* di propaganda politica senza il preventivo consenso del destinatario. L'organo giudicante non ha ritenuto accoglibile l'argomentazione di parte opponente, relativa al fatto che il numero di telefono dell'interessato doveva ritenersi dato conoscibile da chiunque in quanto reperibile *online*, ai sensi dell'art. 24, lett. *c*), del Codice, che costituisce un'eccezione al principio generale dell'obbligatorietà del consenso. In particolare, si è affermato che gli indirizzi di posta elettronica non possono essere qualificati dati "provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque solo perché disponibili nella rete internet" (Trib. Milano, 10 aprile 2014, n. 4882).

Il Tribunale di Milano, con sentenza del 14 maggio 2014, n. 6279, ha accolto il ricorso presentato dal presidente di un'associazione la quale non aveva reso l'informativa e il consenso preventivo in relazione ad una comunicazione a carattere promozionale corredata da pubblicità elettorale. Poiché l'associazione aveva predisposto che tali comunicazioni fossero contenute in buste chiuse e conservate a disposizione degli associati, che potevano prelevarle e distribuirle liberamente, il giudice ha ritenuto non provato che la condotta materiale censurata ed il conseguente evento fossero ascrivibili al suddetto presidente, non potendo, nelle sanzioni amministrative, operare la presunzione di responsabilità per il solo fatto della titolarità dell'organo di rappresentanza, atteso che la responsabilità non può che essere personale e ricollegata alla persona fisica che ha posto in essere la condotta materiale.

Il Tribunale di Reggio Calabria si è soffermato sulla cd. informativa semplificata (cfr. provv. 19 giugno 2008, doc. web n. 1526724) e ha stabilito che non si ravvisano i presupposti per l'applicazione dell'informativa semplificata nell'ipotesi di trattamento dati riguardante soggetti estranei all'organizzazione imprenditoriale, dal momento che non ricorre un trattamento ai sensi dell'art. 34, comma 1-*ter*, del Codice (23 novembre 2012, n. 1864).

In due sentenze il Tribunale di Padova ha ritenuto che l'attivazione di una pluralità di schede telefoniche effettuate da due distinte società nei confronti del singolo interessato senza avergli reso l'informativa, non configuri la violazione dell'art. 13 del Codice, poiché la condotta contestata nel provvedimento impugnato si è concretizzata nel trattamento e utilizzo di dati personali già detenuti dalle predette società, piuttosto che nella raccolta priva di informativa (17 giugno 2014, nn. 2036 e 2037). Avverso tali sentenze il Garante ha proposto ricorso per cassazione.

In alcune sentenze si è affrontato il tema se responsabile dell'illecito amministrativo sia la persona fisica che ha commesso il fatto ovvero anche la persona giuridica.

In un caso una società, che svolgeva attività di portierato e di videosorveglianza per altra compagine sociale, non aveva proceduto alla designazione degli incaricati del trattamento, omettendo di adottare le misure di sicurezza di cui all'art. 33 del Codice. Il giudice, confermando parzialmente il provvedimento del Garante e rideterminando la sanzione al minimo edittale, ha affermato che l'Autorità non è incorsa in errore nel configurare la responsabilità della società opponente con riferimento all'illecito contestato (Trib. Ancona, 3 giugno 2014, n. 973).

In altre due sentenze che avevano ad oggetto, rispettivamente, l'intestazione a persone ignare di utenze telefoniche multiple da parte di un società e l'omessa informativa nella raccolta dati effettuata presso alcuni campeggi da parte di altra società, i giudici, accogliendo i ricorsi, hanno diversamente affermato che il sistema introdotto dalla legge n. 689/1981 è fondato sulla natura personale della responsabilità, per cui autore dell'illecito può essere soltanto la persona fisica che ha commesso il fatto e non anche un'entità astratta per la quale è prevista esclusivamente una responsabilità solidale in funzione di garanzia del pagamento della somma dovuta dall'autore della violazione (Trib. Milano, 18 giugno 2014, n. 8682 e Trib. Venezia, Sez. dist. Portogruaro, 9 luglio 2012, n. 176). Avverso la sentenza del Tribunale di Milano pende ricorso per cassazione proposto dal Garante.

La Cassazione si è pronunciata sull'invio via fax di messaggi di natura promozionale, da parte di una società che non aveva dimostrato di aver reso l'informativa e di avere raccolto un esplicito consenso. La Corte, in linea con quanto a suo tempo deciso dal Garante, dopo aver stabilito che l'utilizzo di un numero di telefono o di fax estratto da un elenco telefonico pubblico debba rientrare nel nozione di trattamento di dati personali, ha escluso che alla vicenda potesse applicarsi la deroga prevista per i soli titolari del trattamento che hanno provveduto a costituire la banca dati prima del 1° agosto 2005, circostanza non riscontrata nel caso considerato; inoltre, tale deroga non opera con riferimento alle comunicazioni promozionali che avvengono senza l'intervento di un operatore, a cui l'invio di fax va assimilato. È stata inoltre respinta anche l'argomentazione circa l'impossibilità di ritenere allo stesso tempo violati l'art. 13 relativo all'omessa informativa e l'art. 23 relativo all'omesso consenso o comunque volta, quand'anche fossero distintamente sanzionabili, all'applicazione del concorso di violazioni continuate, ossia della sanzione più grave aumentata fino ad un terzo. La Cassazione al riguardo ha rilevato che la condotta posta in essere integra due illeciti amministrativi e che la legge n. 689/1981 prevede che la sanzione più grave sia aumentata fino al triplo nei soli casi di concorso formale, senza che possa ritenersi applicabile il medesimo meccanismo sanzionatorio alla fattispecie della continuazione (24 giugno 2014, n. 14326).

In una pronuncia di merito è stato confermato il provvedimento sanzionatorio emesso dal Garante a carico di una società per non aver reso informativa e acquisito il consenso in relazione ad una cessione di dati appartenenti ad altra società. Il giudice ha rilevato che non conoscere il cambio di titolarità del trattamento non consente agli interessati di mantenere un effettivo controllo sui propri dati personali ostacolando di fatto l'esercizio dei diritti di cui all'art. 7 del Codice; ha respinto altresì l'argomentazione secondo la quale, trattandosi di banca dati formata anteriormente al 2005, era applicabile al caso di specie l'esenzione dal consenso di cui all'art. 24 comma 1, lett. *c*), del Codice prevista per i trattamenti commerciali (in quanto riguardano dati provenienti da pubblici registri): ciò perché detta esenzione trova applicazione per i trattamenti eventualmente effettuati dalla società originaria e non già da eventuali società cessionarie come nella fattispecie in esame (Trib. Milano, 11 marzo 2014, n. 5300).

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

In un caso la Cassazione, su ricorso del Garante che si era visto annullare dal Tribunale di Padova un'ordinanza ingiunzione per omessa notificazione emessa nei confronti di un laboratorio di analisi cliniche, ha affrontato il tema dell'errore scusabile ai sensi dell'art. 3, l. n. 689/1981. In primo grado il ricorrente aveva invocato la sussistenza della buona fede di cui al menzionato art. 3 per giustificare l'omessa notificazione, asserendo di essere stato indotto in errore dalla lacunosità della normativa relativamente alla distinzione tra trattamenti esonerati e trattamenti invece soggetti all'obbligo di notificazione. Il Garante infatti con il provvedimento del 31 marzo 2004 (doc. web n. 852561) ha individuato i trattamenti sottratti all'obbligo di motivazione, ai sensi dell'art. 37, comma 2, del Codice.

La Corte ha condiviso l'argomentazione del Garante circa l'insufficienza della motivazione della sentenza di primo grado, che ha completamente ignorato il comunicato del Garante successivo al suddetto provvedimento "nel quale era chiaramente evidenziata la necessità della notificazione per i trattamenti effettuati da strutture sanitarie e, in particolare, per i laboratori analisi clinica e diagnostica per immagine", disponendo la cassazione della sentenza impugnata e il rinvio ad altra sezione del Tribunale (21 gennaio 2014, n. 8030).

Con riferimento ad un'opposizione proposta da una casa di cura avverso un'ordinanza ingiunzione adottata a seguito della violazione dell'obbligo di notificazione al Garante del trattamento di dati sensibili (artt. 37 e ss. del Codice), il Tribunale di Vicenza ha ritenuto che l'attività della casa di cura ricorrente poteva comportare il trattamento di dati sensibili, risultando anche dalla Carta dei servizi che la struttura offre prestazioni in pressoché tutte le branche sanitarie, e tra queste in ambito neurologico e psichiatrico, oltre che tramite un laboratorio convenzionato con il Ssn per analisi chimico cliniche e microbiologiche, diagnosi e trattamento dell'infertilità. Da ciò è apparso evidente che lo svolgimento di tali attività può comportare il rilevamento sia di malattie mentali, infettive o diffusive nonché di dati idonei a rivelare lo stato di salute e la vita sessuale, rendendo quindi necessaria la notificazione, da parte della casa di cura ai sensi dell'art. 37 del Codice (cfr. Cass., Sez. VI, 8 aprile 2014, n. 8184). Diversamente opinando, ritenendo che la notificazione sia necessaria solo per le attività di rilevamento svolta in via principale per scopi scientifici (secondo l'orientamento espresso da Trib. Chiavari, 12 giugno 2012 e Trib. Ravenna, 8 novembre 2012), si verrebbe a disapplicare, ha sottolineato il Tribunale, la disciplina del Codice proprio in relazione alle strutture sanitarie che maggiormente rilevano e trattano dati sensibili, ponendo nel nulla la *ratio* della normativa in materia di protezione dei dati personali. Secondo il Tribunale, peraltro, non poteva essere invocata da parte dell'opponente neanche la buona fede, visto che il Garante ha più volte chiarito, con varie deliberazioni e circolari, che solo i medici persone fisiche sono esentati dall'obbligo di notifica e non le strutture come le case di cura e ciò è stato reso esplicito dall'inserimento nell'art. 37 del Codice del comma 1-*bis*, inserito dall'art. 2-*quinquies*, d.l. n. 81/2004 (28 ottobre 2014, n. 2270).

In altro caso simile sempre la Cassazione ha respinto il ricorso di una casa di cura sanzionata dal Garante per aver ritardato la comunicazione di inizio dell'attività di trattamento dei dati idonei ad identificare malattie ereditarie e quelli relativi alla procreazione, rientranti nella disposizione prevista dall'art. 37 del Codice. La casa di cura opponente, che, in forza di un contratto di affitto di azienda, aveva acquisito la disponibilità dei dati personali da altra società (la quale aveva già provveduto ad effettuare la notificazione al Garante), aveva sostenuto la non necessità della comunicazione al Garante dell'inizio del trattamento dei dati sensibili, visto che il legale rap-

presentate era la medesima persona fisica per entrambe le società, coincidendo anche la sede. La Cassazione ha confermato la sentenza di primo grado e il provvedimento del Garante, osservando che, ai sensi dell'art. 28 del Codice, titolare del trattamento è la persona giuridica e non il legale rappresentate o l'amministratore unico quale organo della società; pertanto il subentro nella gestione di un'azienda nel campo sanitario che tratta dati di natura comune e sensibile dei propri pazienti, di altra società avente distinta persona giuridica determina l'obbligo di effettuare la notificazione al Garante ai sensi dell'art. 37 del Codice (18 marzo 2014, n. 8184).

In un'altra pronuncia una società è stata sanzionata per aver omesso di notificare al Garante la cessazione del trattamento a seguito del passaggio della titolarità del medesimo trattamento ad altra società del gruppo, pur nella coincidenza della persona fisica titolare, degli organi di rappresentanza e degli uffici utilizzati da entrambi gli enti, elementi non sufficienti, secondo il giudice, a ritenere l'esistenza di un'unica soggettività giuridica, posta la formale indipendenza giuridica delle società del gruppo (Trib. Milano, 23 dicembre 2013, n. 15735).

Alcune pronunce hanno riguardato provvedimenti in materia del giornalismo.

In un primo caso il Tribunale di Roma ha confermato la decisione del Garante 12 luglio 2012 (doc. web n. 1925739) in merito alla pubblicazione su un sito internet di alcuni articoli relativi a controversie giudiziarie intentate dai ricorrenti.

L'organo giudicante, dopo aver rilevato che il procedimento davanti al Garante era stato svolto correttamente, poiché non vi è alcun obbligo di fissare una successiva audizione ai sensi dell'art. 149, comma 3, del Codice, qualora, come nel caso di specie, l'audizione precedentemente fissata fosse andata deserta, ha ritenuto che il trattamento dati nella vicenda in esame fosse espressione del diritto di manifestazione del pensiero, nel rispetto dei principi di essenzialità dell'informazione, pertinenza e interesse pubblico alla notizia (2 aprile 2014, n. 7789).

In altro caso il giudice, confermando la decisione del Garante, ha ritenuto che la pubblicazione di una rettifica sul sito web di un quotidiano, concernente un articolo nel quale, per ragioni di omonimia, era stato erroneamente indicato un nome e pubblicata un'immagine non corretti, avesse posto rimedio all'illecito ed erroneo trattamento di dati, eliminandone gli effetti; sono state altresì condivise le argomentazioni del Garante che aveva respinto la richiesta di eliminazione dell'articolo in questione dall'archivio ritenendo che tale pubblicazione avesse finalità storiche e non costituisse nuova pubblicazione né ulteriore illecito trattamento di dati personali (Trib. Milano, 11 ottobre 2011, n. 12004).

Con pronuncia del 17 febbraio 2014, n. 16494, il Tribunale di Milano ha affrontato un caso di pubblicazione di due articoli sul sito web di un quotidiano dei quali il ricorrente, in qualità di erede dell'interessato, aveva chiesto la rimozione ovvero, in via subordinata, che venissero resi anonimi i dati personali in esso contenuti ed in via ulteriormente subordinata venissero aggiornate le notizie. In una articolata motivazione, oltre a confermare la legittimità del provvedimento opposto, il giudice di merito ha trattato in maniera diffusa la questione del bilanciamento tra diritto all'informazione e tutela della riservatezza. Preliminarmente è stata considerata la questione della legittimazione, rilevando che il diritto alla riservatezza si estingue con la morte del titolare, sopravvivendo una forma di tutela di dati sensibili, quali l'accesso ai dati a tutela del defunto o per ragioni familiari meritevoli di protezione secondo quanto stabilito dall'art. 9 del Codice e confermato da una pronuncia del Consiglio di Stato (12 giugno 2012, n. 3459), per cui se non può invocarsi il diritto all'oblio da parte dell'erede, deve invece ammettersi la richiesta di rettificazione o cancellazione di dati falsi, non esatti o non aggiornati. Quanto alla vicenda, l'organo giudicante ha dichiarato la cessazione della materia del con-

tendere in ordine a tutte le domande aventi ad oggetto un primo articolo, in quanto era stato deindicizzato da parte della società editrice che aveva provveduto altresì ad un aggiornamento riportando in calce al suddetto articolo l'esito del procedimento giurisdizionale, restando sospesa la sola questione della rimozione del secondo articolo, che pure era stato deindicizzato. A tal proposito è stata richiamata una recente pronuncia della Cassazione, la quale ha affermato che il diritto all'oblio, declinato nel controllo della notizia a tutela della propria immagine sociale, anche quando trattasi di notizia vera e di cronaca, può tradursi nella pretesa alla contestualizzazione, aggiornamento e anche cancellazione dei dati (Cass. civ., 11 gennaio 2012, n. 5525: cfr. par. 20.3). In linea con tale giurisprudenza, in due provvedimenti del 2013, il Garante ha sostenuto che la tutela dell'interessato viene garantita dal diritto ad ottenere l'aggiornamento e l'integrazione dei dati personali quando siano intervenuti fatti nuovi che incidano in modo significativo sul riflesso che ne deriva all'onore e alla reputazione dell'interessato e all'identità sociale che da essi promana, ai sensi dell'art. 7 del Codice. In applicazione dei principi suddetti, il Tribunale di Milano ha ritenuto che per il mero trascorrere del tempo o la morte del titolare non venga meno l'interesse alla conoscenza del dato di cronaca, essendo necessario valutare nel caso concreto se la compressione del diritto alla reputazione dell'interessato comporti un sacrificio non giustificato dal corrispondente interesse alla conoscenza del dato da parte della collettività. In conclusione è stato confermato il provvedimento del Garante, che aveva rigettato la richiesta volta ad ottenere la cancellazione ovvero l'aggiornamento dei dati, poiché gli articoli di stampa nascevano come espressione di libera manifestazione del pensiero ed erano legittimamente conservati per finalità di documentazione all'interno di un archivio: ciò in quanto nella vicenda in esame, non poteva contestarsi il potenziale interesse alla conoscenza della vicenda peraltro derivante da attività di cronaca giudiziaria legittimamente esercitata che aveva ad oggetto l'attività imprenditoriale del defunto (17 febbraio 2014, n. 16494).

La Corte di Cassazione è intervenuta in una controversia relativa alla pubblicazione di un servizio fotografico su un settimanale che riportava immagini relative a momenti di vita privata quotidiana di alcuni soggetti.

Il Garante, con provvedimento del 23 novembre 2005 (doc. web n. 1200112), accogliendo le doglianze dei segnalanti, aveva ritenuto che il trattamento dati fosse stato effettuato in violazione dei limiti dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico.

La Corte, dopo aver ribadito che l'attività giornalistica è sottoposta al rispetto del relativo codice di deontologia oltre che del Codice, le cui norme sono volte a contemperare la libertà di stampa con i diritti fondamentali della persona, tra cui quello alla riservatezza, ha affermato che la divulgazione di un dato di interesse pubblico mediante dichiarazioni o comportamenti pubblici da parte degli stessi interessati non è configurabile come forma di consenso tacito al suo trattamento, poiché la deroga all'art. 137, ultimo comma, del Codice concerne l'essenzialità del dato trattato e non l'interesse pubblico, che va apprezzato autonomamente ai fini della trattabilità del dato per finalità giornalistiche in contesti diversi dalla loro originaria pubblicazione (18 ottobre 2013, n. 27381).

In un caso, una banca ha impugnato il provv. 21 dicembre 2011 (doc. web n. 1877695) che le ordinava di mettere a disposizione di un dipendente, destinatario di sanzioni disciplinari, i dati personali allo stesso non trasmessi attinenti al procedimento che ne era stato alla base. Il giudice ha confermato il provvedimento suddetto, ritenendolo coerente con i principi in tema di difesa nel procedimento disciplinare e nel giudizio (Trib. Roma, 28 gennaio 2014, n. 21769).

Con riguardo, invece, all'invio da parte di un comune dell'intero fascicolo del procedimento disciplinare aperto nei confronti di un dipendente al Collegio dei geometri, trattandosi di professionista iscritto all'albo, il Tribunale di Busto Arsizio ha confermato il provvedimento del Garante che aveva respinto il ricorso proposto dal dipendente. In particolare, il Tribunale, nel ricordare quanto sancito dall'art. 19, comma 2, del Codice, ha sottolineato come nel caso in esame la trasmissione dei documenti fosse avvenuta "per lo svolgimento di funzioni istituzionali", in quanto finalizzata a segnalare al Collegio in questione una violazione di legge da parte di un iscritto all'Albo, non quale lavoratore alle dipendenze di una pubblica amministrazione, ma quale libero professionista tenuto al rispetto del codice deontologico della propria categoria professionale (5 ottobre 2014, n. 1716).

Due sentenze hanno affrontato la questione relativa alla somministrazione di *test* ai candidati alla selezione di un dirigente tecnico da inserire nell'organico di un ente, effettuata per conto di quest'ultimo, da una società. Le opposizioni sono state proposte con due distinti ricorsi rispettivamente dall'ente committente e dalla società selezionatrice, nei confronti del relativo provvedimento del Garante.

La Corte di Cassazione, in sintonia con il suddetto provvedimento, ha confermato che tra la società incaricata di procedere alla procedura di selezione in esame e l'ente a favore del quale la selezione veniva effettuata sussisteva un'ipotesi di cotitolarità del trattamento dati, in quanto la società aveva direttamente proceduto alla somministrazione dei questionari, mentre l'ente aveva concorso a determinare le finalità e le modalità del trattamento, occupandosi della complessiva organizzazione. Il provvedimento del Garante è stato condiviso anche per quanto concerne l'omessa informativa che avrebbe dovuto essere fornita successivamente al primo contatto, in quanto trattavasi di *curricula* inviati su iniziativa dell'interessato a seguito di annuncio di lavoro, non potendosi peraltro neppure applicare la normativa più favorevole intervenuta successivamente alla commissione del fatto con l'introduzione del comma 5-*bis* all'art. 13 del Codice, poiché in tema di illeciti amministrativi vige il principio dell'assoggettamento alla legge del tempo del loro verificarsi (5 giugno 2014, n. 12707 e 11 giugno 2014, n. 13219).

Un'ulteriore pronuncia ha respinto il ricorso avverso un provvedimento del Garante in materia di videosorveglianza sul luogo di lavoro. Nel caso in esame, un esercizio commerciale deteneva le immagini registrate dall'impianto di videosorveglianza per un periodo di tempo pari a cinque giorni, mentre il provvedimento autorizzativo della Direzione provinciale del lavoro prevedeva un temine massimo di 24 ore. Il giudice, a fronte dell'argomentazione proposta dalla ricorrente circa la possibilità di deroga al limite delle 24 ore per il rischio relativo all'integrità del patrimonio aziendale, ha ritenuto che la possibilità di deroga riguardi esclusivamente il profilo del contemperamento tra le esigenze di sicurezza e quelle di riservatezza, ma non anche il profilo afferente alla tutela della dignità dei lavoratori. Pertanto, nell'ipotesi in cui dall'installazione di impianti audiovisivi derivi un controllo a distanza sull'attività lavorativa, in assenza di accordo con le rappresentanze sindacali, le immagini debbono essere conservate in conformità ai tempi stabiliti dalle direzioni territorialmente competenti (Trib. Bolzano, 3 luglio 2014, n. 826).

La Corte di Cassazione è altresì intervenuta, su ricorso del Garante che si era visto annullare dal Tribunale di Verbania il provvedimento con il quale aveva fatto divieto all'Amministrazione di trattare le informazioni acquisite dal web relative alla vita sessuale di un proprio dipendente, poste alla base di un provvedimento di destituzione dal lavoro. La Cassazione ha annullato la sentenza di primo grado e confermato il provvedimento del Garante, osservando che il Codice, in riferimento ai dati sensibili, comprendenti in particolare quelli idonei a rivelare lo stato di

salute e la vita sessuale dell'interessato, ne consente il trattamento per lo svolgimento di compiti istituzionali da parte di un soggetto pubblico, senza necessità del consenso e dell'autorizzazione del Garante, solo se autorizzato da un'espressa disposizione di legge in cui devono essere specificati i tipi di dati che possono essere trattati, i tipi di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite, ovvero in base ai regolamenti *ad hoc* adottati dalle singole Amministrazioni su parere conforme del Garante.

Il regolamento adottato dall'Amministrazione aveva individuato i tipi di dati trattabili e le operazioni eseguibili ai fini dell'instaurazione e della gestione del rapporto di lavoro, da una parte, e ai fini della gestione del contenzioso dall'altra, prevedendo che il trattamento dei dati relativi alla vita sessuale fosse consentito senza limitazione solo nel secondo caso, mentre nel primo caso solo in casi di rettificazione del sesso.

La Cassazione ha rilevato che il dato oggettivo dell'acquisizione delle informazioni attinenti alla vita sessuale del dipendente fosse di per sé un'attività sufficiente a configurare un trattamento di dati sensibili, da valutare con riguardo alla gestione del rapporto di lavoro. Pertanto, non trattandosi di un'ipotesi di rettificazione di attribuzione di sesso, è stata esclusa la legittimità del trattamento, respingendo la tesi dell'Amministrazione circa la riconducibilità del trattamento in esame alla gestione del contenzioso, che invece presuppone una diretta connessione con una controversia già in essere.

Infine, è stata respinta anche l'argomentazione della ricorrente che riteneva che l'immissione in rete di alcuni dati personali da parte dell'interessato (nella specie, sotto forma di diffusione di annunci) implicasse la volontà di rivolgersi ad un pubblico indeterminato, con la conseguente impossibilità di garantire la limitata diffusività degli annunci. La Cassazione ha invece affermato, con richiamo di precedenti, che non può ritenersi che quel consenso sia stato prestato implicitamente in funzione di qualsiasi altro trattamento (7 ottobre 2014, n. 21107).

Vi sono infine decisioni relative a materie diverse ed eterogenee.

Una di esse ha riguardato un'istanza di accesso alla cartella clinica di una neonata, deceduta presso la struttura ospedaliera subito dopo la nascita, effettuata dalla madre naturale che si è avvalsa del diritto a non essere nominata previsto dall'art. 30, comma 1, d.P.R. n. 392/2000.

È stato riconosciuto dal giudice il diritto anche per la madre naturale di ottenere l'accesso ai dati personali richiesti, in quanto agiva ai sensi dell'art. 9, comma 3, del Codice, e dunque a tutela dell'interessato o per ragioni familiari meritevoli di protezione; in particolare nel caso in esame vi era l'esigenza di accertare la patologia genetica di cui la madre avrebbe potuto essere portatrice e le modalità della sua trasmissione, così da poterle consentire una valutazione del rischio procreativo e una scelta riproduttiva consapevole ed informata (Trib. Napoli, 18 settembre 2014, n. 13212).

Un caso ha riguardato una segnalazione pregiudizievole da parte di un istituto di credito alle banche dati di settore, in presenza di un accordo transattivo, in cui gli istituti di credito rinunciavano a parte delle loro ragioni di credito, a seguito della contestazione da parte di clienti e intermediari di condotte illegittime degli stessi istituti.

Il giudice, annullando il provv. 20 dicembre 2012, n. 436 (doc. web n. 2375765), ha ritenuto che qualunque segnalazione a centrale pubblica o privata, anche nel caso di transazione, deve presupporre una situazione di insolvenza in relazione all'entità del debito, al tempo trascorso nello stato di insolvenza e alla volontà di non adempiere, elementi che non si sono ritenuti sussistere nel caso di specie (Trib. Roma, 23 ottobre 2013, n. 21191).

Ha trovato conferma un provvedimento del Garante che ha ravvisato l'illegittimità e la non correttezza del trattamento di dati personali da parte di una società che si occupa della ricerca di un impiego, in quanto gli interessati, per potersi candidare alle offerte di lavoro presenti sul sito internet, dovevano acconsentire al trattamento dei propri dati personali per finalità ulteriori e diverse, ossia all'invio di offerte commerciali da parte della società in questione e di terzi soggetti non individuati. Il Tribunale ha confutato, tra gli altri, l'argomento sollevato dalla società ricorrente secondo cui l'attività svolta dalla stessa rientrerebbe nella deroga di cui all'art. 24, comma 1, lett. *b*), del Codice per cui il consenso non è necessario quando il trattamento "è necessario per eseguire obblighi derivanti da un contratto". Nella fattispecie, ha precisato il giudice, è indubitabile, infatti, che il servizio offerto dalla società ricorrente era quello di informare gli interessati rispetto a possibili offerte di lavoro, essendo solamente questa la prestazione contrattuale richiesta ed attesa dai fruitori del sito (Trib. Como, 16 settembre 2014, n. 1531).

In un'altra vicenda, il Tribunale di Venezia ha respinto l'impugnazione avverso un provvedimento del Garante di illiceità del trattamento svolto da una compagnia telefonica attraverso l'utilizzo dei dati personali dei segnalanti per finalità di comunicazioni promozionali in assenza del prescritto riscontro presso il registro pubblico delle opposizioni e tramite chiamate prive dell'identificazione della linea chiamante. Trattandosi di comunicazioni finalizzate alla commercializzazione, è risultata l'illiceità del trattamento in quanto il consenso non era stato specificato e documentato per iscritto, come prescritto dall'art. 23 del Codice, né raccolto previa idonea informativa, come richiesto dall'art. 13 del Codice stesso (17 ottobre 2014, n. 2177).

È stato altresì ritenuto inammissibile il ricorso in Corte di Cassazione avverso la sentenza del Tribunale di Ferrara che aveva respinto l'impugnazione del provv. 26 luglio 2006 (doc. web n. 1323119) con cui veniva vietato l'utilizzo dei dati personali dei ricorrenti da parte dei titolari di un'agenzia assicurativa, a fini promozionali, rigettando però la richiesta di cancellazione dei dati formulata solo con ricorso al Garante ai sensi dell'art. 146 del Codice e non preceduta dall'interpello *ex* art. 7 dello stesso Codice. Si evidenzia in particolare che dalla lettura della sentenza impugnata risulta che erano state fatte telefonate promozionali agli interessati da persona che affermava di ricordare nomi e i numeri dei clienti dell'agenzia. Sul punto la Corte afferma che il Garante non aveva contraddittoriamente ordinato di non trattare dei dati a chi quei dati non deteneva, come lasciato intendere dalla ricorrente, avendo invece ritenuto che nell'ampia nozione di trattamento di cui all'art. 4, d.lgs. cit. fosse possibile ricomprendere ogni possibile operazione su dati di clienti o di terzi che un'azienda, un ente o un diverso tipo di organizzazione detiene, a prescindere dal tipo di organizzazione (informatizzata o meno) predisposta dal titolare. Verrebbe quindi sostanzialmente fatto rientrare nella nozione di trattamento anche il caso di chi utilizza dei dati ricordandoli a memoria (cfr. Cass., Sez. VI, 10 marzo 2014, n. 5452).

21.5. *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.

Era stato invece spiegato intervento, in grado di appello, avverso una sentenza del Tar Lazio (14 agosto 2013, n. 9036) che aveva accolto il ricorso contro il diniego tacito opposto dall'Agenzia delle Entrate ad un'istanza di accesso, presentata dal coniuge del soggetto cui i dati reddituali si riferivano, per utilizzare i dati stessi nel procedimento giudiziale di separazione.

Nella specie l'istanza riguardava, tra l'altro, le comunicazioni di cui all'art. 7, d.P.R. n. 605/1973, come modificato dal d.l. 4 luglio 2006, n. 223, convertito con modificazioni dalla legge 4 agosto 2006, n. 248, in base al quale sussiste l'obbligo per ogni operatore finanziario di comunicazione, in un'apposita sezione dell'Anagrafe tributaria, denominata Archivio dei rapporti finanziari, dell'esistenza e relativa natura dei rapporti finanziari intrattenuti con qualsiasi soggetto.

La sentenza era stata impugnata dal Garante insieme con l'Agenzia delle Entrate, rappresentando, tra l'altro, che le comunicazioni in parola, una volta riversate nell'Archivio dei rapporti finanziari da parte delle banche e degli operatori finanziari, possono essere utilizzate "unicamente" dall'Amministrazione finanziaria e dalla Guardia di finanza, e, comunque, che le norme in parola autorizzano l'accesso agli atti *de quibus* nella sola forma della "visione".

Al riguardo il Consiglio di Stato (14 maggio 2014, n. 2472) ha ritenuto la cura e la tutela degli interessi economici e della serenità dell'assetto familiare, soprattutto nei riguardi dei figli minori delle parti in causa, prevalenti "o quantomeno da contemperare con il diritto alla riservatezza previsto dalla normativa vigente in materia di accesso a tali documenti «sensibili» del coniuge" e "dirimente, al riguardo, il fatto che nella specie la richiesta di accesso sia provenuta dal marito della controinteressata, e non da un *quisque de populo*, e che l'interesse dello stesso, attuale e concreto, alla cura dei propri interessi in giudizio si presentasse sicuramente qualificato", condividendo perciò le valutazioni del primo giudice. Alla luce della disposizioni in parola ha però accolto l'appello sul punto relativo alla limitazione dell'accesso alla sola visione delle comunicazioni in questione.

È giunto a conclusione anche un altro giudizio nel quale era intervenuto il Garante, relativo alle modalità di notificazione di un'ordinanza-ingiunzione emessa per la violazione di un'ordinanza sindacale volta a contrastare il fenomeno della prostituzione su strada. Il Garante era intervenuto nel giudizio intentato dall'interessato per chiedere al comune il risarcimento del danno allo scopo di tutelare aspetti di interesse generale, segnatamente evidenziando che la notificazione dell'atto presso un domicilio diverso da quello eletto dall'interessato avrebbe potuto rilevare sul piano della protezione dei dati personali.

La Cassazione, con sentenza del 5 settembre 2014, n. 18812, in una complessa decisione, pur senza dar conto di quanto prospettato dal Garante, ha affermato (tra l'altro) che i danni cagionati per effetto del trattamento dei dati personali in base all'art. 15 del Codice sono assoggettati alla disciplina di cui all'art. 2050 c.c., con la conseguenza che il danneggiato è tenuto solo a provare il danno e il nesso di causalità con l'attività di trattamento dei dati, mentre spetta al convenuto la prova di aver adottato tutte le misure idonee ad evitare il danno.

Nella specie, la Corte ha confermato la decisione di merito che aveva escluso la sussistenza della prova liberatoria in relazione all'illegittimo trattamento dei dati –

consistito nella propalazione delle circostanze fattuali in cui era maturata l'infrazione amministrativa presupposto dell'ingiunzione, e cioè la violazione di ordinanza sindacale volta a contrastare il fenomeno della prostituzione su strada – avvenuto da parte del comune mediante la notifica del provvedimento a mezzo dei messi comunali, senza avvalersi della possibilità di notifica nel domicilio eletto dall'interessato nel procedimento amministrativo, ovvero presso lo studio del suo difensore.

Quanto al risarcimento, peraltro, la Corte ha cassato senza rinvio – per mancata prova del danno da parte dell'interessato – la decisione di I grado che lo aveva accordato.

22 L'attività ispettiva e le sanzioni

22.1. *La programmazione dell'attività ispettiva*

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

Le ispezioni (385 nel 2014) sono effettuate sulla base di programmi ispettivi elaborati secondo linee di indirizzo stabilite dal Collegio con delibere di programmazione che indicano gli ambiti del controllo e gli obiettivi numerici da conseguire. Le linee generali della programmazione dell'attività ispettiva vengono quindi rese pubbliche attraverso il sito web del Garante e, sulla base dei criteri così fissati, l'Ufficio individua i titolari dei trattamenti da sottoporre a controllo e istruisce i conseguenti procedimenti. Il programma ispettivo relativo al 2014 ha previsto che la relativa attività fosse, tra l'altro, indirizzata nei seguenti settori:

- grandi banche dati pubbliche: per controllare i trattamenti di dati personali effettuati 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 questi archivi di rilevanti dimensioni gestiti da soggetti pubblici avvenga solo ed esclusivamente nel rispetto dei presupposti fissati dal legislatore e che vengano costantemente aggiornate le misure per prevenire violazioni della sicurezza dei dati;
- *Internet eXchange Point* (IXP): per verificare le principali misure adottate dalle società che gestiscono i primari nodi nazionali di interscambio del traffico internet, al fine di garantire la sicurezza dei dati degli utenti/interessati;
- strutture sanitarie: per rilevare l'impostazione dei trattamenti di dati personali effettuati in relazione all'istituzione del Fascicolo sanitario elettronico (Fse) e del *dossier* sanitario, che rappresentano i moderni strumenti di raccolta e di condivisione delle informazioni e dei documenti clinici;
- *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*. Questa attività si inserisce organicamente nel complesso di iniziative istruttorie con le quali l'Autorità si è proposta 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 quotidiani *online*, libri elettronici, giochi, ecc. pagando con il credito telefonico): per verificare la correttezza dei trattamenti di dati personali effettuati da tutti i soggetti coinvolti nelle transazioni effettuate mediante tali sistemi (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 dei beni digitali, cd. *merchant*);

- 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, il Garante, oltre ad analizzare la liceità e la correttezza dei trattamenti effettuati, si è riproposto di valutare l'attualità delle prescrizioni già adottate;
- trasferimento di dati personali in Paesi extra-UE: per verificare la liceità dei trattamenti in ordine al trasferimento dei dati personali verso Paesi terzi (extra-UE) tra società facenti parte di un medesimo gruppo sulla base di clausole vincolanti d'impresa (cd. *Binding corporate rules* – Bcr);
- banche dati utilizzate per il *marketing:* per controllare i trattamenti di dati personali effettuati da società che gestiscono grandi banche dati per finalità di *marketing.*

Come specificato al par. 22.3, nel periodo di riferimento sono state anche effettuate verifiche in altri settori concernenti:

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

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

22.2. *La collaborazione con la Guardia di finanza*

L'Autorità continua ad avvalersi della preziosa collaborazione della Guardia di finanza per lo svolgimento dell'attività di controllo in applicazione del protocollo di intesa siglato nel 2005 (cfr. in merito, quanto nel dettaglio riferito nelle precedenti edizioni e, da ultimo, nella Relazione 2009, p. 240). 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.

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

Grazie alla sinergia ormai collaudata con il Nucleo speciale *privacy*, il Garante dispone di un dispositivo di controllo flessibile ed articolato, in grado di integrare l'attività ispettiva svolta direttamente dal competente Dipartimento dell'Autorità, consentendo così l'effettuazione, efficace e tempestiva, delle verifiche *in loco* che si rendono necessarie per garantire il rispetto della protezione dei dati personali sull'intero 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: in questa cornice, sono stati organizzati due seminari presso il Nucleo speciale *privacy* nell'ambito dei quali sono stati esaminati vari profili relativi ai procedimenti sanzionatori e illustrato il provvedimento generale in tema di biometria del 12 novembre 2014, n. 513 (doc. web n. 3556992) e le allegate Linee guida.

Considerati gli ottimi risultati raggiunti nel rapporto di collaborazione ormai ultradecennale tra il Garante e la Guardia di finanza e al fine di tenere conto delle nuove sfide tecnologiche nonché del rilievo sempre maggiore che l'ambito internazionale avrà nelle istruttorie anche a seguito della definizione del nuovo quadro normativo europeo, sono stati avviati contatti volti a realizzare, nell'anno 2015, un aggiornamento del protocollo d'intesa tra le due Istituzioni.

22.3. *I principali settori oggetto di controllo*

Oltre a quanto riferito al par. 22.1, le ispezioni effettuate dall'Autorità nel 2014 hanno riguardato i titolari del trattamento che:

- operano nel settore delle biotecnologie, per rilevare le modalità e le finalità del trattamento dei dati personali degli interessati, le misure di sicurezza adottate, l'eventuale profilazione, nonché le modalità con cui viene resa l'informativa e raccolto il consenso degli interessati. Le verifiche sono state orientate ad appurare altresì l'eventuale comunicazione di dati a terzi o il trasferimento degli stessi in Paesi extra-UE;
- operano nel settore dell'assistenza tecnica/manutenzione e del recupero dati, relativamente ad apparecchiature informatiche o telefoniche, per verificare gli accorgimenti adottati per assicurare la tutela dei dati dei clienti memorizzati su detti dispositivi, con particolare riferimento alle misure di sicurezza predisposte nonché ai presupposti giuridici, all'ambito e alle modalità dell'eventuale comunicazione a terzi dei dati;
- forniscono servizi di intermediazione immobiliare, per verificare la liceità del trattamento dei dati dei clienti raccolti attraverso siti web oppure attraverso le agenzie. In particolare, le verifiche sono state indirizzate prevalentemente nei confronti di gruppi immobiliari di rilevante dimensione (operanti sia con una propria rete di vendita diretta che attraverso sistemi di *franchising*), per appurare le modalità di acquisizione dei dati personali della clientela e i flussi di dati tra i diversi attori coinvolti (gruppo societario, società partecipate, agenzie, *franchisor*, *franchisee* ed interessati);
- forniscono servizi di comunicazione elettronica accessibili all'utenza 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 provv. 17 gennaio 2008 (doc. web n. 1482111). Tra questi vanno ricordati: 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;

- operano nel settore del credito, per verificare il trattamento di dati personali relativi all'utilizzo di impianti di videosorveglianza, sia di tipo tradizionale che di tipo integrato con la rilevazione di dati biometrici della clientela (tratti dall'analisi delle impronte digitali). In tali casi le verifiche si sono incentrate sull'utilizzo di sistemi di videosorveglianza, per accertare il rispetto di quanto prescritto dal Garante nell'ambito del provvedimento generale in materia di videosorveglianza dell'8 aprile 2010 (doc. web n. 1712680); sull'utilizzo di sistemi di videosorveglianza integrati con la raccolta delle impronte digitali della clientela, al fine di verificare, in particolare, la sussistenza dei presupposti di liceità del trattamento e l'adozione delle misure di tutela previste dal provvedimento generale 27 ottobre 2005 (doc. web n. 1246675), tra cui: nomina del "vigilatore" dei dati, ottenimento dell'attestato di conformità di cui alla regola n. 25 dell'All. B al Codice, rispetto dei tempi massimi di conservazione e delle procedure di cancellazione automatica dei dati, adozione di sistemi di cifratura "robusti", affissione di una informativa "minima" all'esterno dell'agenzia, effettiva predisposizione di modalità alternative di accesso per la clientela;
- sviluppano o distribuiscono applicazioni per dispositivi mobili di comunicazione (cd. *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'istallazione 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;
- operano avvalendosi dell'attività degli informatori scientifici del farmaco, per verificare, in particolare: l'origine dei dati personali relativi agli operatori sanitari contattati dalle cause farmaceutiche attraverso gli informatori scientifici, le modalità di raccolta degli stessi, l'eventuale profilazione, le modalità di rilascio dell'informativa e di acquisizione del consenso, nonché la titolarità delle banche dati costituite attraverso l'espletamento della suddetta attività. Tali verifiche, tuttora in corso, coinvolgono anche gli stessi informatori scientifici, sia nel caso in cui questi collaborino con la società farmaceutica in virtù di uno specifico mandato di agenzia, che nel caso in cui siano dipendenti della società stessa;
- gestiscono concessionarie "plurimarca" per la vendita di motoveicoli od operano nel settore del commercio elettronico (*e-commerce*), al fine di appurare il rispetto della disciplina con particolare riferimento ai profili dell'informativa resa agli interessati nonché del consenso dagli stessi manifestato, ove necessario;
- operano nel settore della compravendita di metalli preziosi o gioielli (cd. compro oro), 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;
- operano nel settore alberghiero con strutture di categoria elevata o di lusso, al fine di verificare la liceità del trattamento dei dati della clientela, anche con riferimento ai dati raccolti attraverso siti web o attraverso l'utilizzo di sistemi di videosorveglianza, con particolare evidenza per le modalità di rilascio dell'informativa e di raccolta del consenso degli interessati, ove necessario;
- operano nel settore dei laboratori di analisi cliniche. In tal caso le verifiche hanno riguardato, oltre al rispetto delle disposizioni del Codice concernenti il rilascio dell'informativa, la raccolta del consenso e la notificazione del trattamento, anche l'analisi delle misure di sicurezza adottate per la protezione dei dati sensibili presenti presso i laboratori e di quelle predisposte per consentire agli interessati l'accesso ai propri dati personali via internet o per le comunicazioni attraverso l'uso della posta elettronica.

Particolarmente rilevante, per complessità e significatività di risultato, è stata l'attività condotta nei confronti dei principali nodi d'interscambio internet (*Internet eXchange Point*-IXP). I nodi di interscambio (d'ora in poi IXPs) sono infrastrutture fisiche che permettono a diversi internet *Service Providers* (ISPs) di scambiare traffico internet fra loro, interconnettendo le proprie reti IP (*Internet Protocol*) attraverso cd. accordi di *peering* (nelle reti informatiche, *peering* è l'interconnessione volontaria tra reti internet che siano distinte amministrativamente allo scopo di scambiare traffico fra gli utenti di entrambe). Questo consente agli ISPs risparmi sugli acquisti di banda trasmissiva fornita dagli *upstream provider* e maggiore efficienza e affidabilità.

In estrema sintesi, lo scopo principale di un IXP è di permettere alle reti degli ISPs, attraverso il punto di interscambio neutrale, di interconnettersi fra di loro direttamente, senza passaggi intermedi, piuttosto che far transitare il traffico attraverso uno o più *provider* esterni. Oltre agli evidenti benefici economici e gestionali, la connessione diretta tra gli operatori tramite un IXP diminuisce la "distanza" tra le reti degli ISPs nazionali (intesa quale numero di passaggi per connettere un ISP ad un altro), evitando che l'interconnessione avvenga, come spesso accade, al di fuori del territorio nazionale, con l'effetto di migliorare il servizio reso all'utenza internet poiché i tempi di latenza nelle comunicazioni basate su protocollo Ip tra utenti (aziende, individui) basati sul territorio nazionale saranno in genere inferiori, rendendo la fruizione dei servizi di rete più efficiente e rapida. Gli accordi di *peering* tra i partecipanti ad un nodo di interscambio sono per lo più effettuati a titolo gratuito e regolati in modo da garantire il rispetto del principio di neutralità dell'attività dell'IXP nei confronti degli afferenti.

L'attività di controllo nei confronti degli IXPs si inquadra nelle attività di controllo che l'Autorità effettua per verificare il rispetto delle disposizioni del Codice che disciplinano le comunicazioni elettroniche. Le ispezioni hanno messo in luce rilevanti criticità con riferimento a diversi profili attinenti la sicurezza.

Come richiesto dall'Autorità a seguito delle ispezioni, gli IXPs hanno introdotto adeguati sistemi di tracciamento delle attività svolte dai tecnici sugli apparati, in modo da rilevare eventuali anomalie, come la possibile deviazione o duplicazione del traffico internet, oppure il collegamento di altri apparati elettronici alla rete interna; hanno eliminato le credenziali tecniche "condivise", così da poter identificare con certezza le attività svolte dal singolo operatore o amministratore di sistema e adottato meccanismi di *audit* e *alert* per prevenire o scoprire eventuali attività "ostili"; hanno migliorato, inoltre, la sicurezza fisica dei locali, essendo stato rafforzato il controllo degli accessi e la sorveglianza dei locali tecnici, con particolare

attenzione anche alle infrastrutture e ai *data center*. Per quanto riguarda questo ultimo aspetto, l'Autorità ha raccomandato, agli IXPs che hanno parte dei loro apparati dislocati in *data center* esterni, di operare controlli attivi e regolari sulle strutture che li ospitano.

Il Garante, consapevole del fatto che la sicurezza delle comunicazioni elettroniche coinvolge le competenze anche di altri soggetti istituzionali, ha dato notizia delle attività svolte al Presidente del Consiglio, trasmettendo altresì il rapporto ispettivo, affinché fosse valutato dagli organismi preposti alla sicurezza cibernetica del Paese (nota 26 maggio 2014). Alla segnalazione del Garante ha fatto seguito un'attività del Nucleo per la sicurezza cibernetica della Presidenza del Consiglio dei ministri, nell'ambito della quale sono state individuate plurime linee di azione per aumentare la sicurezza delle reti.

Sono stati effettuati altresì controlli nei confronti di singoli 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.

22.4. *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 del caso, a uno o più dei seguenti obiettivi:

- intervenire sui trattamenti illeciti da chiunque effettuati adottando i provvedimenti cautelari previsti dalla legge (blocco e divieto) e/o definendo le misure necessarie da prescrivere per rendere il trattamento conforme alla legge (contrasto dell'illecito);
- verificare lo stato di attuazione delle prescrizioni adottate dal Garante nei diversi contesti e sanzionare gli eventuali inadempimenti al fine di prevenire futuri illeciti (attività preventiva);
- acquisire tutti gli elementi utili a comprendere nuovi fenomeni emergenti suscettibili di incidere significativamente sul diritto alla protezione dei dati personali (ad es., il tema del *mobile remote payment*) in modo da definire tempestivamente misure e accorgimenti da adottare (attività conoscitiva).

Occorre tenere presente che, al di là della/e finalità che la sottendono, l'ispezione è comunque pur sempre un procedimento amministrativo di controllo all'esito del quale, ove vengano accertate illiceità, l'Autorità è tenuta ad adottare i necessari provvedimenti per rendere il trattamento conforme alla legge e a contestare le sanzioni eventualmente rilevate.

Con riferimento al 2014, tra i provvedimenti più rilevanti adottati 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 effettuato mediante un sistema di videosorveglianza 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 9 gennaio 2014, n. 13, doc. web n. 2927804 e 4 dicembre 2014, n. 559, doc. web n. 3671057);
- rilevato l'illiceità del trattamento effettuato dalla Società italiana di nefrologia per l'alimentazione del Registro italiano di dialisi e trapianto in man-

canza dell'informativa e del consenso dei pazienti interessati (artt. 13, 23, 106, 107 e 110 del Codice) e vietato all'associazione medesima di effettuare per il futuro ulteriori trattamenti di dati personali anche attinenti alla salute, salva l'adozione delle misure necessarie indicate dal Garante (provv. 16 gennaio 2014, n. 16, doc. web n. 2937031);

- dichiarato illecito il trattamento dei dati personali di imprese e professionisti effettuato da una società che inviava fax promozionali, senza la preventiva acquisizione del necessario consenso libero, informato, specifico e documentato per iscritto *ex* artt. 23, comma 3 e 130, commi 1 e 2, del Codice (provv. 23 gennaio 2014, n. 30, doc. web n. 2927848);
- disciplinato il fenomeno delle cd. chiamate mute, nelle quali cioè la persona contattata, dopo aver attivato il ricevitore, non viene messa in comunicazione con alcun interlocutore, e la cui ricezione reiterata e continua, a volte anche per dieci - quindici volte di seguito e spesso protratta nel tempo, determina un particolare disturbo ai destinatari ai quali, in difetto appunto di interlocutore, sono preclusi tutele e rimedi. Il provvedimento, avente carattere generale, prescrive ai titolari del trattamento che utilizzano i *call center* misure atte a minimizzare questo fenomeno (provv. 20 febbraio 2014, n. 83, doc. web n. 3017499);
- impartito 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 conservati per finalità di accertamento e repressione dei reati (cd. *data retention*), già prescritti dall'Autorità con il provv. generale 17 gennaio 2008 (doc. web n. 1482111), successivamente integrato con il provv. generale 24 luglio 2008 (doc. web n. 1538237) (provv.ti 20 febbraio 2014, n. 84, doc. web n. 3031194 e 20 marzo 2014, n. 137, doc. web n. 3136961);
- prescritto a un'azienda sanitaria le misure per rendere conformi al Codice i trattamenti effettuati dagli interessati in relazione alle operazioni di pagamento dei corrispettivi per le prestazioni sanitarie dalla stessa erogate attraverso la rete Sportello amico di Poste Italiane s.p.a. e tramite il proprio sito internet (provv. 13 marzo 2014, n. 120, doc. web n. 3041470);
- prescritto ai titolari che effettuano trattamenti di dati personali nell'ambito delle operazioni di *mobile remote payment*, le misure per effettuare tali trattamenti nel rispetto dei principi generali di liceità, pertinenza, non eccedenza, correttezza e buona fede di cui all'art. 11 del Codice (provv. 22 maggio 2014, n. 258, doc. web n. 3161560);
- ritenuto illecito il trattamento effettuato da una società a mezzo del sistema di localizzazione dei veicoli aziendali volto a migliorare la qualità del servizio, a gestire i reclami degli utenti nonché a ottemperare a quanto richiesto da una regione in sede di affidamento del servizio, che consentiva altresì di effettuare il controllo a distanza dell'attività dei dipendenti che prestano servizio a bordo dei veicoli aziendali, senza che fossero attivate le procedure previste dall'art. 4, comma 2, l. 20 maggio 1970, n. 300; sono state inoltre prescritte le misure per rendere il trattamento conforme al Codice (provv. 2 ottobre 2014, n. 434, doc. web n. 3534543);
- rilevato l'illiceità del trattamento effettuato da due aziende sanitarie con riferimento all'omessa informativa e alla mancata acquisizione del consenso dell'interessato in relazione al trattamento dei dati dei pazienti effettuato

tramite il *dossier* sanitario aziendale (artt. 13, 23 e 76 e ss. del Codice), vietato ulteriori trattamenti di dati personali mediante lo strumento del *dossier* sanitario aziendale e prescritto le misure necessarie per rendere il trattamento dei dati conforme al Codice (provv.ti 23 ottobre 2014, n. 468, doc. web n. 3570631; 18 dicembre 2014, n. 610, doc. web n. 3725976);

- dichiarato illecita la raccolta dei dati personali degli utenti effettuata da una società sul proprio sito web e mediante moduli cartacei per le attività di invio di comunicazioni promozionali per conto proprio e/o per conto terzi nonché di comunicazione dei dati raccolti a soggetti terzi per le loro finalità promozionali (o comunque per finalità diverse da quelle strumentali ovvero collegate all'erogazione del servizio o dell'esecuzione del contratto), senza aver provveduto alla previa acquisizione del necessario consenso, *ex* art. 23, comma 3, del Codice; vietato il trattamento dei dati raccolti in violazione del Codice e prescritto alla medesima società le misure necessarie e opportune al fine di rendere il trattamento dei dati personali conforme alle disposizioni del Codice (provv. 20 novembre 2014, n. 532, doc. web n. 3657934).

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.

22.5. *L'attività sanzionatoria del Garante*

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

Nel 2014, in relazione alle istruttorie effettuate, sono state inviate 39 segnalazioni di violazioni penali all'autorità giudiziaria (cfr. sez. IV, tab. 7) di cui:

- venti per la mancata adozione delle misure minime di sicurezza;
- sette per violazioni della l. n. 300/1970 (Statuto dei lavoratori), ora punite come reato dall'art. 171 del Codice;
- due per falsità nelle dichiarazioni e notificazioni al Garante;
- una per trattamento illecito dei dati;
- una per inosservanza di un provvedimento del Garante;
- otto in relazione ad altre violazioni penali.

Come dimostrano i dati sopra riportati, permangono numerose le violazioni delle misure minime di sicurezza; ciò nonostante si tratti di adempimenti di non particolare complessità, in vigore da più di dieci anni, che dovrebbero essere stati oramai "metabolizzati" sia dalle imprese che dagli enti pubblici. Anche alla luce dell'esperienza maturata dall'Autorità in sede di controllo 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. 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. In questo senso, in data 22 settembre 2014 (doc. web n. 3531329), l'Autorità ha fatto una segnalazione al Presidente del Consiglio dei

ministri nell'ambito di una articolata proposta di semplificazione del quadro sanzionatorio e delle misure minime di sicurezza previste dal Codice (cfr. par. 22.7).

Al di là dei risvolti sanzionatori, occorre sottolineare che la mancata osservanza delle disposizioni relative alle misure minime di sicurezza è particolarmente grave perché espone i dati personali degli interessati al pericolo di accesso da parte di persone non autorizzate e a trattamenti non consentiti.

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

In questo ambito merita segnalare la recente sentenza della Corte di Cassazione (Sez. pen., III, 16 gennaio 2015, n. 1986) che ha affrontato, respingendola, la questione di legittimità costituzionale dell'art. 169 del Codice, in riferimento agli artt. 2, 3, 21, 24, 25 della Costituzione. Nella motivazione si legge che "non sussiste, infatti, alcun contrasto di tale disposizione con gli artt. 3 e 24 Cost., perché rientra in generale nella piena discrezionalità del legislatore la fissazione dell'ammontare dell'oblazione ai fini dell'estinzione del reato, come avvenuto, attraverso il richiamo all'art. 162, comma 2-*bis*, in ragione di euro 30.000".

Nella stessa sentenza la Suprema Corte afferma, con riferimento alla responsabilità penale, che la stessa "è stata, del resto, positivamente accertata dalla Guardia di finanza nel corso delle indagini preliminari, attraverso l'accertamento diretto della mancata designazione dell'incaricato del trattamento in relazione ad un sito internet nel quale era possibile la raccolta di dati personali sensibili relativi a una serie indeterminata di persone", confermando la linea costantemente seguita negli anni dall'Autorità circa le conseguenze penali derivanti dall'omessa designazione degli incaricati del trattamento dei dati.

Anche nel 2014 si è avuta una rilevante incidenza dell'accertamento di violazioni penali relative allo Statuto dei lavoratori connesse, nella maggior parte dei casi, all'installazione di sistemi di videosorveglianza in assenza delle garanzie previste dall'art. 4, comma 2, l. n. 300/1970. Occorre tenere presente che la disciplina prevista dallo Statuto e relativa all'utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori (art. 4) e al divieto di indagini sulle opinioni ai fini dell'assunzione (art. 8), costituisce parte integrante delle disposizioni del Codice (artt. 113 e 114) ed è sanzionata dall'art. 171.

22.5.2. Le sanzioni amministrative

Sono stati avviati n. 577 nuovi procedimenti sanzionatori amministrativi (cfr. sez. IV, tab. 6). All'accertamento delle violazioni amministrative previste dal Codice può procedere:

- il personale dell'Ufficio addetto all'attività ispettiva a cui, sulla base di quanto previsto dall'art. 156, comma 9, del Codice, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, è attribuita la qualifica di ufficiale o agente di polizia giudiziaria;
- chiunque rivesta, nell'esercizio delle proprie funzioni, la qualifica di ufficiale o agente di polizia giudiziaria, in base a quanto previsto dall'art. 13, l. 24 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 ecc. che possono accertare le violazioni amministrative in materia di protezione dei dati personali in occasione di attività svolte sulla base dei propri poteri, anche di polizia giudiziaria. Questo "doppio binario" risulta complessivamente efficace, considerata l'amplissima platea di soggetti tenuti all'osservanza delle regole previste dal Codice, che renderebbe velleitario un sistema di accertamento delle violazioni accentrato solo nell'Autorità.

L'assicurazione di una uniformità di giudizio e di interpretazione è peraltro assicurata, in quanto la legge affida 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 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 2014 hanno riguardato:

- l'omessa o inidonea informativa – art. 161 (n. 228);
- il trattamento illecito amministrativo – art. 162, comma 2-*bis* (n. 171);
- l'omessa comunicazione all'interessato, circa l'avvenuta violazione dei dati personali, da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico (cd. *data breach*) – art. 162-*ter*, comma 2 (n. 92);
- 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 o incompleta notificazione – art. 163 (n. 16);
- l'omessa adozione delle misure minime di sicurezza di cui all'art. 33 del Codice – art. 162, comma 2-*bis* (n. 15);
- 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. 14);
- l'omessa informazione o esibizione al Garante – art. 164 (n. 14);
- l'inosservanza di un provvedimento del Garante – art. 162, comma 2-*ter* (n. 6);
- l'omessa comunicazione al Garante, circa l'avvenuta violazione dei dati personali, da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico (cd. *data breach*) – art. 162-*ter*, comma 1 (n. 2).

Un approfondimento merita il dato relativo alle 171 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 previsioni del Codice, estremamente eterogenee, e, in particolare, gli artt.: 17 (verifica preliminare), 18, 19, 20, 21, 22, commi 8 e 11 (disposi-

zioni 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 2014 le violazioni concernenti il "trattamento illecito amministrativo" accertate hanno riguardato:

- in 101 casi, la violazione del consenso dell'interessato in rapporto agli artt. 23 e 130 del Codice;
- in 29 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 14 casi, violazioni delle misure e degli accorgimenti prescritti dal Garante nell'ambito di una verifica preliminare sulla base dell'art. 17 del Codice;
- in 14 casi, violazioni commesse da enti pubblici con riferimento a dati sensibili;
- in 5 casi, violazioni commesse da fornitori di reti pubbliche di comunicazione o di servizi di comunicazione elettronica con riferimento ai dati di traffico di abbonati o utenti;
- in 2 casi, violazioni commesse da soggetti privati in relazione al trattamento di dati sensibili o giudiziari;
- in 2 casi, violazioni commesse da fornitori di reti pubbliche di comunicazione o di servizi di comunicazione elettronica con riferimento all'inserimento e all'utilizzo dei dati personali relativi agli abbonati negli elenchi pubblici, cartacei o elettronici;
- in un caso, una violazione commessa in relazione al trasferimento di dati personali in Paesi extra-UE;
- in un caso, una violazione commessa da un ente pubblico con riferimento a dati 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 del consenso dell'interessato (n. 101) 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 120 violazioni accertate rispetto a 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;
- si sono verificati i primi casi di violazioni relative all'omessa comunicazione all'interessato e al Garante, circa l'avvenuta violazione dei dati personali, da parte di fornitori di servizi di comunicazione elettronica accessibili al pubblico (cd. *data breach*); in uno dei due casi, oltre alla mancata comunicazione del *data breach* al Garante è stata anche rilevata e contestata la mancata comunicazione ai diretti interessati (92 persone) i cui dati erano stati indebitamente violati.

I procedimenti sanzionatori definiti nel 2014 con provvedimento di ordinanza ingiunzione adottato dall'Autorità, relativamente a violazioni contestate negli anni precedenti al 2014 e non definite all'epoca attraverso il pagamento spontaneo in misura ridotta da parte del contravventore, sono stati 270. Di questi, 202 hanno comportato l'applicazione di una sanzione (per un ammontare complessivo di somme ingiunte pari a 1.953.000 euro) e 68 si sono invece conclusi con l'archiviazione in quanto la parte ha potuto dimostrare nel procedimento di non aver commesso la violazione contestata o che la violazione non era ad essa imputabile.

Tra le ordinanze più rilevanti adottate si segnalano quelle relative a violazioni dell'obbligo di informativa e di acquisizione del consenso degli interessati per l'utilizzo dei dati per finalità di *marketing;* in questi provvedimenti, essendo i dati destinati a confluire all'interno di banche dati di particolare rilevanza e dimensioni, è stata applicata anche la sanzione prevista dall'art. 164-*bis*, comma 2, del Codice (ordinanza ingiunzione 8 maggio 2014, n. 231, doc. web n. 3275922; ordinanza ingiunzione 2 ottobre 2014, n. 437, doc. web n. 3747707; ordinanza ingiunzione 12 novembre 2014, n. 519, doc. web n. 3685448)

Per quanto invece riguarda i profili giuridici di maggiore interesse, si possono prendere in esame, in particolare, i seguenti casi:

- raccolte dati *online* per le quali la casella relativa al consenso al trattamento è pre-impostata per raccogliere il consenso in violazione dell'art. 23 del Codice. Per effetto di quanto previsto dall'art. 23 del Codice, il consenso al trattamento dei dati, per essere acquisito legittimamente, deve sempre essere, oltre che informato, anche libero. Relativamente a tale requisito essenziale, le manifestazioni del consenso rese obbligatorie mediante la pre-impostazione di *flag*, siano essi modificabili che non modificabili, non consentono il lecito trattamento dei dati raccolti per finalità ulteriori rispetto a quella per la quale il *form* di raccolta è preposto, così come peraltro più volte asserito dall'Autorità in diversi provvedimenti (già con provv. 10 maggio 2006, doc. web n. 1298709, e più di recente, tra gli altri, con provv. 4 luglio 2013, n. 330, doc. web n. 2542348) (ordinanze ingiunzione 18 dicembre 2014, n. 612, doc. web n. 3745935 e n. 613, doc. web n. 3750400);
- effetti della scadenza dei termini nel procedimento amministrativo con riferimento al distinto procedimento sanzionatorio dei cui alla l. n. 689/1981. Benché la l. n. 241/1990 sul procedimento amministrativo stabilisca, all'art. 2, il generale principio del dovere di rispettare il termine di conclusione del procedimento amministrativo, nessuna disposizione di legge lo ha elevato a requisito di validità dell'atto amministrativo. Pertanto, anche la violazione di un termine indicato dai Regolamenti del Garante nn. 1 e 2/2007 non vizia l'atto amministrativo (verbale di contestazione), sopravvenuto alla scadenza di un termine del procedimento cui tale atto è riferibile. Partendo da questo presupposto, la contestazione delle sanzioni amministrative accertate dal Garante in un suo provvedimento non è viziata, a condizione che sia rispettato il termine previsto dall'art. 14, l. n. 689/1981 (cfr. ordinanza ingiunzione del 12 novembre 2014, n. 520, doc. web n. 3624070);
- sanzionabilità delle telefonate promozionali effettuate oscurando il numero del chiamante. La condotta consistente nell'effettuazione di chiamate telefoniche promozionali camuffando o celando l'identità del chiamante ovvero senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'art. 7 del Codice, sostanzia un illecito amministrativo riconducibile alla previsione di cui all'art. 130, comma 5, del Codice e sanzionata dall'art. 162, comma 2-*quater* in combinato disposto con gli artt. 162,

comma 2-*bis* e 167 del Codice. Ne consegue che l'invio di comunicazioni a scopo promozionale, previsto nel comma 5, si riferisce all'utilizzo di un qualsiasi mezzo, tra quelli previsti nei primi tre commi dell'art. 130, per l'effettuazione di comunicazioni promozionali, quindi anche alle chiamate con operatore (ordinanza ingiunzione 22 maggio 2014, n. 263, doc. web n. 3276281);

- autonoma valenza, quale fattispecie sanzionatoria, dell'illecito di cui all'art. 164-*bis*, comma 2, del Codice. L'Autorità, tornando ad affrontare e approfondire le tematiche relative alla sanzione sulle grandi banche dati, nel ribadire (cfr. Relazione annuale 2013) "i criteri in base ai quali le banche dati in questione possono essere definite di particolare rilevanza, indipendentemente dalla numerosità del *database*, o dimensione, in ragione della quantità di dati in esso contenuti", ha asserito, trovando poi conforto nella sentenza dell'11 marzo 2014, del Tribunale di Milano – I Sez. civ., il principio secondo cui la violazione di cui all'art. 164-*bis*, comma 2, del Codice configura una "fattispecie complessa", collegata ma autonoma rispetto a quelle presupposte. Una pluralità di violazioni commesse in relazione a banche dati di particolari dimensioni o rilevanza, determina un'offesa a un bene giuridico ulteriore rispetto a quello inciso dalle singole violazioni (che costituiscono il presupposto dell'illecito di che trattasi), in ragione del maggiore pregiudizio che si sostanzia quando i dati vengono aggregati all'interno di una banca dati con le specifiche peculiarità (banche dati di eccezionale dimensione o rilevanza) costituenti il presupposto dell'illecito in questione (ordinanze ingiunzione 8 maggio 2014, n. 231, doc. web n. 3275922; 2 ottobre 2014, n. 437, doc. web n. 3747707 e 12 novembre 2014, n. 519, doc. web n. 3685448).

Pagamenti effettuati

L'ammontare dei pagamenti effettivamente effettuati nel 2014 da parte dei soggetti nei cui confronti sono stati avviati procedimenti sanzionatori amministrativi è risultato complessivamente pari a 4.907.866 euro (cfr. sez. IV, tab. 8), di cui:

- 2.374.135 euro, pagati a titolo di definizione in via breve;
- 1.968.136 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;
- 445.595 euro, quali ulteriori entrate derivanti dall'attività sanzionatoria (ad es., riscossione coattiva).

Gli importi relativi alle sanzioni applicate dal Garante sono versati sul bilancio dello Stato. Sulla base di quanto previsto dall'art. 166 del Codice, tali proventi, nella misura del 50% del totale annuo, sono riassegnati al fondo stanziato per le spese di funzionamento dell'Autorità previsto dall'art. 156, comma 10, del Codice e utilizzabili unicamente per l'esercizio della attività ispettiva e di divulgazione della disciplina della protezione dei dati personali.

22.6. *Le novità introdotte nel 2014 relativamente ai procedimenti sanzionatori*

Nell'ottica del continuo miglioramento delle attività procedimentali, nel 2014 sono state individuate alcune soluzioni che consentiranno di aumentare l'efficienza dell'Ufficio e, contemporaneamente, di semplificare gli adempimenti dei destinatari dei provvedimenti con riferimento al pagamento delle sanzioni amministrative. Tali profili riguardano:

- l'indicazione di un unico riferimento di conto a livello nazionale sul quale devono essere effettuati tutti i pagamenti (anziché tanti riferimenti quante sono le tesorerie provinciali, in funzione della residenza del contravventore);
- la ricezione dalla Ragioneria generale dello Stato, con cadenza mensile, di una reportistica contenente l'indicazione e tutti gli estremi dei versamenti contabilizzati sul capo X, capitolo 2373 del bilancio dello Stato ove affluiscono i pagamenti delle sanzioni in materia di protezione dei dati personali (precedentemente l'Ufficio non aveva invece alcuna evidenza di tali versamenti).

Per quanto riguarda il primo aspetto, l'aver individuato la Tesoreria provinciale di Roma quale unico ente presso cui far confluire tutti i pagamenti eviterà il dover riportare, di volta in volta, codici Iban e numeri di conto corrente postale diversi in ragione della residenza del contravventore.

Quanto al secondo aspetto, si potranno ottenere ulteriori miglioramenti:

- un maggiore controllo sui pagamenti: precedentemente il controllo dell'effettivo pagamento delle sanzioni era estremamente complesso. L'Ufficio doveva infatti basarsi sulla ricezione dei versamenti effettuati (mediante bonifici bancari o postali) e non aveva modo di verificarli se non richiedendo un riscontro all'intermediario utilizzato dalla parte per il pagamento. Con la ricezione del flusso informativo da parte della Ragioneria generale dello Stato invece si ha una rendicontazione verificata e attendibile dei versamenti effettivamente effettuati;
- una maggiore completezza e precisione nella rendicontazione dell'attività sanzionatoria: i dati sui pagamenti effettuati precedentemente avrebbero potuto essere (in parte) sottostimati, potendo sfuggire alcuni pagamenti; il sistema precedente non consentiva di disporre con precisione dei dati relativi ai versamenti effettuati dai contravventori in un dato periodo temporale. Nelle comunicazioni della Ragioneria generale dello Stato sono presenti anche i versamenti che vengono effettuati da Equitalia in ragione delle somme derivanti da ordinanze ingiunzione non pagate ed iscritte a ruolo. Tali somme, di cui precedentemente non si aveva evidenza, contribuiscono a definire l'ammontare degli incassi sul capitolo 2373 del Capo X del bilancio dello Stato. È così più agevole, alla fine dell'anno, disporre di un rendiconto puntuale di tutte le somme incassate;
- eliminazione della procedura di verifica sull'eventuale pagamento: in tutti i casi nei quali agli atti non risultava il pagamento né l'invio da parte del contravventore di memorie difensive, prima di procedere a predisporre l'ordinanza, l'Ufficio inviava una lettera tipo per verificare l'eventuale pagamento della sanzione evitando così di dover poi eventualmente revocare l'ordinanza adottata. Tale procedura non è adesso più necessaria.

Con l'invio, da parte della Ragioneria generale dello Stato, del riepilogo mensile dei versamenti effettuati (descritti precedentemente), l'Ufficio dispone adesso di dati "certificati" che rendono del tutto superfluo l'invio della contabile a dimostrazione dell'assolvimento dell'obbligo di pagamento.

Sono state pertanto modificate le istruzioni che vengono comunicate al contravventore, abolendo l'obbligo di trasmissione delle quietanze di pagamento, alleggerendo le incombenze e riducendo notevolmente i flussi documentali, specie nei casi di pagamenti rateali.

Per agevolare e orientare tutti i soggetti coinvolti nei procedimenti sanzionatori è stata infine realizzata e pubblicata sul sito una nuova sezione informativa contenente le risposte ai questi più frequenti.

22.7. *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*

Come anticipato (crf. par. 22.5.1), il Garante ha suggerito al Governo alcune modifiche all'attuale apparato sanzionatorio con l'invio al Presidente del Consiglio dei ministri della comunicazione denominata: "Semplificazione del quadro sanzionatorio e delle misure minime di sicurezza previste dal Codice" (nota 22 settembre 2014, doc. web n. 3531329), rinnovando l'invito anche in tempi successivi (nota 16 gennaio 2015).

Nella lettera, il Presidente dell'Autorità rappresenta che: "Le misure prospettate potrebbero assicurare significativi benefici, anche in termini economici, soprattutto alle piccole e medie imprese o comunque ai soggetti, anche pubblici, di modeste dimensioni, senza tuttavia abbassare lo *standard* delle garanzie per i cittadini e nel rispetto dei vincoli dell'Unione europea".

Il progetto di riforma del quadro giuridico in materia di protezione dei dati, infatti, si sostanzia in alcuni interventi mirati di modifica del Codice ispirati ai seguenti principi:

- semplificazione del quadro sanzionatorio e aumento dell'equità nell'applicazione delle sanzioni, mediante, fra l'altro, la ridefinizione dei confini tra le fattispecie penali e amministrative e la limitazione della responsabilità penale per la mancata adozione delle misure minime di sicurezza ai soli casi in cui ne sia derivata una conseguenza negativa nella sfera giuridica degli interessati;
- riduzione dei costi diretti e indiretti (di consulenza e assistenza legale) per i soggetti destinatari di sanzioni, mediante il ricorso diretto e automatico a modalità di estinzione agevolata dei procedimenti sanzionatori e diminuendo i casi in cui non è ammessa l'estinzione mediante oblazione;
- promozione di un aggiornamento delle misure minime di sicurezza previste dal Codice (art. 36) anche con disposizioni differenziate in ragione dei rischi effettivi per i diritti degli interessati e minimizzando l'impatto economico delle stesse, in particolare presso le piccole e medie imprese, liberi professionisti e artigiani. A tal fine, si prevede la consultazione delle categorie interessate e si affida al Garante il compito di proporre tali adempimenti sulla base dell'esperienza maturata dalla quotidiana applicazione delle relative disposizioni.

Queste modifiche appaiono ancora oggi necessarie e utili nell'ottica di bilanciare ulteriormente un assetto che, nell'esperienza quotidiana dell'Autorità, appare talvolta eccessivamente gravoso 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 par. 22.5.1, ormai indifferibile appare la revisione delle misure minime di sicurezza contenute nel disciplinare tecnico All. 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 fre-

quenti) in cui lo stesso è oggetto di trasferimenti per mezzo delle reti di comunicazione o di accesso da parte di postazioni remote.

Tale esigenza appare ancora più evidente se si considera che, sulla base dell'attività esercitata quotidianamente dall'Autorità e di studi condotti da osservatori indipendenti, sussistono ancora carenze non trascurabili nei livelli di sicurezza garantiti dalle pubbliche amministrazioni rispetto ai dati trattati nei loro sistemi informativi. Tali carenze assumono una rilevanza ancora maggiore se si tiene presente l'accelerazione registrata negli ultimi tempi nel processo di informatizzazione della p.a., che ha determinato l'esigenza di correggere la crescente asimmetria tra la capacità d'innovazione tecnologica e gli *standard* di sicurezza adottati dalle Istituzioni.

D'altro canto, non meno rilevante appare tale esigenza in riferimento alle misure di sicurezza adottate dagli operatori privati. La collocazione non adeguata delle problematiche relative alla sicurezza dei dati personali nell'ambito delle priorità e degli investimenti operati da soggetti privati, specie se di grandi dimensioni, contribuisce alla mancata percezione degli aspetti connessi alla protezione, integrità e sicurezza dei dati quali fattori strategici di competitività, innovazione e *accountability* per le imprese, traducendosi in ultima istanza in un più generale limite allo sviluppo del Paese (con risvolti negativi, a volte, sull'intera sicurezza nazionale, come nel caso degli IXPs).

Il mancato aggiornamento delle misure minime di sicurezza contenute nel disciplinare tecnico All. B al Codice, durante questi anni, è certamente imputabile, almeno in parte, alle modalità con le quali tale procedimento di revisione deve realizzarsi ai sensi dell'art. 36 del Codice, ovvero con 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 (A.S. 958), 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.

23 Le relazioni comunitarie e internazionali

Nonostante le aspettative, il 2014 non ha portato, a livello europeo e internazionale, al completamento dei lavori per l'adozione dei nuovi strumenti legislativi in materia di protezione dei dati personali. Si tratta com'è noto della revisione della Convenzione n. 108/1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale e delle proposte di regolamento e di direttiva che formano il pacchetto per un nuovo quadro giuridico europeo in materia di protezione dei dati.

Nel Consiglio d'Europa, il CAHDATA – comitato intergovernativo incaricato dal Comitato dei ministri di portare a termine il processo di modernizzazione della Convenzione 108, sulla base della proposta del Comitato T-PD – ha concluso il proprio mandato con l'adozione a dicembre 2014 del documento contenente la Convenzione modernizzata. Tuttavia, sul testo adottato dal CAHDATA, continuano a pesare le riserve della Commissione europea su alcuni articoli che corrispondono a nodi non ancora sciolti nell'ambito del nuovo regolamento UE (vedi par. 23.1).

In ambito UE, analogamente, sebbene sia la 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) che la proposta di direttiva sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e proseguimento di reati o esecuzioni di sanzioni penali (doc. web n. 2110225), volta a sostituire la Decisione quadro 977/2008 (relativa al trattamento dei dati personali trattati nell'ambito della cooperazione di polizia e giudiziaria in materia penale), siano state adottate in prima lettura, con emendamenti, dal Parlamento europeo, non sono stati portati a termine i lavori presso il Consiglio UE che deve ancora addivenire ad una propria posizione comune (v., in proposito, par. 23.1).

In sede OCSE, è proseguito il lavoro di revisione delle Linee guida sicurezza dell'OCSE del 2002 *(Recommendation Concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security)* che andranno ad affiancare le nuove Linee guida *privacy* dell'OCSE, adottate nel 2013 (cfr. Relazione 2013, p. 189).

Il Garante ha continuato ad impegnarsi per poter contribuire attivamente a tali processi di riforma partecipando ai diversi gruppi e comitati di lavoro istituiti, in particolare attraverso gli sforzi profusi nel semestre di Presidenza italiana dell'UE per cercare di far progredire i lavori sui testi in discussione presso il Consiglio (per una versione d'insieme v. sez. IV, tab. 25).

Il 2014 si è caratterizzato invece per l'intensificarsi delle attività di cooperazione – tema al centro dei lavori della Conferenza di primavera dei Garanti europei – tra le autorità di protezione dei dati europee (soprattutto con riferimento ai trattamenti di dati effettuati dalle multinazionali che operano *online*) e anche a livello internazionale (cfr. par. 23.2).

Contributi importanti per chiarire il quadro applicativo della disciplina in materia di protezione dei dati sono inoltre pervenuti dalla Corte di giustizia che si è espressa con importanti sentenze sulla nozione di stabilimento e sul diritto alla deindicizzazione dai motori di ricerca (cfr. par. 23.3, doc. web n. 3127044), sull'indi-

pendenza delle autorità di protezione dei dati (doc. web n. 3845166), sulla direttiva che imponeva l'obbligo di conservazione dei dati di traffico telefonico e telematico per finalità di polizia (cd. *data retention*) (doc. web n. 3043705: cfr. par. 23.3) e sulla definizione del concetto di trattamento di dati per finalità strettamente personali (doc. web n. 3845146: cfr. par. 14.5,).

Il tema della sorveglianza ha continuato ad essere al centro della riflessione delle autorità di protezione dei dati. In particolare, le autorità europee di protezione dei dati – riunite nel Gruppo Art. 29, del quale nel 2014 il presidente Antonello Soro è stato eletto vice-presidente – hanno adottato una dichiarazione comune volta a riaffermare i valori condivisi a livello europeo e a proporre alcune azioni concrete al fine di sviluppare un quadro di principi per una *governance* europea democratica e rispettosa dei diritti fondamentali. La dichiarazione, presentata in occasione del *European data governance forum* tenutosi a Parigi l'8 dicembre 2014 (v. par. 23.2), richiama la responsabilità di tutti i soggetti, privati e pubblici, affinché sia assicurato il rispetto di tali principi, specie nella raccolta ed utilizzo dei dati personali nell'economia digitale.

23.1. *La riforma del quadro giuridico europeo in materia di protezione dei dati*

Dopo che, il 12 marzo 2014, il Parlamento europeo ha votato la propria posizione in prima lettura, la pressione affinché il Consiglio UE terminasse l'analisi del "pacchetto" protezione dati si è fatta indubbiamente più forte. Colloqui interistituzionali necessari a mettere a punto un testo di compromesso (attraverso il cd. "trilogo" fra Parlamento, Commissione e Consiglio UE) potranno infatti iniziare soltanto quando il Consiglio avrà raggiunto, su entrambe le proposte legislative, un accordo sulla propria posizione negoziale. La Presidenza greca e, quindi, quella italiana hanno dato un forte impulso ai lavori del competente gruppo di lavoro (DAPIX) giungendo, per quanto riguarda in particolare la proposta di regolamento, ad un cd. "accordo generale parziale" su alcuni elementi importanti: art. 1 (Oggetto e obiettivi); art. 3 (Campo di applicazione territoriale); art. 4, limitatamente alla definizione di "stabilimento principale" e di "*Binding corporate rules*"; art. 6 (Liceità del trattamento); art. 21 (Limitazioni alle disposizioni del Regolamento); capo IV (Obblighi dei titolari e responsabili di trattamento, artt. 22-39-*bis*); capo V (Trasferimenti internazionali di dati, artt. 40-45); capo IX (artt. 80-85 - Disposizioni relative a particolari tipologie di trattamento: per finalità giornalistiche, esercizio libertà di espressione, accesso a documenti pubblici, contesto lavorativo, archivi, trattamenti scientifici, statistici, storici, norme in materia di riservatezza professionale, confessioni religiose). È stato, inoltre, ottenuto dai Ministri UE durante il Consiglio GAI di dicembre 2014 un sostanziale *endorsement* per l'architettura generale del meccanismo di "sportello unico" (*One-Stop-Shop*, capi VI e VII: artt. 46-72), così come rielaborato dalla Presidenza italiana (v. *infra*).

Il Garante ha partecipato costantemente alle riunioni del DAPIX ed ha intensificato la propria collaborazione, in particolare con la Presidenza italiana del secondo semestre del 2014, fornendo proprie analisi e formulando osservazioni e proposte anche alla luce dei pareri e dei documenti adottati in materia dal Gruppo Art. 29 (v. Relazione 2013).

Guardando agli elementi oggetto di accordo per quanto concerne la proposta di regolamento, vale la pena di sottolineare, in particolare, gli ulteriori margini di flessibilità introdotti per gli Stati membri attraverso l'art. 1. In base al testo modificato sotto la Presidenza italiana, essi saranno autorizzati a "introdurre o mantenere"

disposizioni che specifichino ulteriormente quelle contenute nel regolamento per i trattamenti svolti "nel pubblico interesse", in aggiunta alle disposizioni di deroga (già previste dagli artt. 6 e 21, e modellate su quelle contenute anche nell'attuale direttiva 95/46/CE, soprattutto dall'art. 13 di quest'ultima). Numerosi Stati membri hanno, infatti, chiesto di poter disporre di un maggiore margine di "flessibilità", indipendentemente dalla natura pubblica o privata del titolare di trattamento, per consentire soluzioni anche più stringenti rispetto ai requisiti del regolamento, nel presupposto di un pubblico interesse da perseguire (quest'ultimo definito in modo più specifico attraverso un apposito "considerando").

Importante anche l'accordo sul tema (orizzontale) del cd. approccio basato sul rischio del trattamento, tale da calibrare gli obblighi del titolare sul rischio che ciascun trattamento comporta, e che si inquadra nel contesto più ampio del principio di *accountability* (responsabilizzazione dei titolari di trattamento). Il testo approvato dai ministri durante il Consiglio GAI di ottobre 2014 individua il livello di rischio su cui ponderare gli obblighi dei titolari (rischio "elevato"), definendo (in via generale) i fattori da tenere in considerazione (art. 22) e quindi declinando l'approccio "basato sul rischio" in varie disposizioni (artt. 23, 26, 28, 30, 31, 33 e 34); queste ultime mirano essenzialmente a fornire indicazioni su natura, contesto, campo di applicazione, scopi dell'attività di trattamento dei dati e sui rischi esistenti per i diritti e le libertà degli interessati. Ad esempio, il trattamento di dati pseudonimizzati (che restano dati personali, come precisato in un apposito considerando) viene ritenuto utile a ridurre il rischio del trattamento, mentre l'obbligo di notifica all'autorità di controllo delle violazioni relative ai dati personali, esteso dalla proposta di regolamento a tutti i titolari di trattamento (artt. 31 e 32), è stato riformulato in chiave di rischio per evitare eccessivi oneri amministrativi e, per altro verso, un eccesso di notifiche per violazioni alle Autorità garanti. Rientrano in quest'ambito anche la valutazione di impatto (obbligatoria) e la consultazione preventiva dell'autorità di controllo (artt. 33 e 34), per cui si prevede l'obbligo per i titolari di consultare l'autorità solo nei casi in cui l'esito della valutazione di impatto si concluda con il riconoscimento di un rischio "elevato" nonostante le misure di mitigazione del rischio adottate dal titolare; fra queste ultime si ricordano, in particolare, la nomina di un DPO (*Data Protection Officer*, o "incaricato della protezione dati") (artt. 35-37), che il documento propone come facoltativa in via generale, l'adozione (e l'osservanza) di specifici codici deontologici settoriali, anche europei (art. 38 e 38-*bis*), il rilascio di certificazioni anche su base europea (art. 39 e 39-*bis*), con intervento delle autorità di protezione dati al fine di "certificare i certificatori". A tale proposito, il Gruppo Art. 29 aveva sottolineato (in uno "*Statement*" pubblicato sul punto nel mese di maggio 2014, WP 218, doc. web n. 3815164) la necessità di interpretare il concetto di "rischio" guardando all'intero impatto che il trattamento di dati personali può determinare sugli interessati (quindi anche sulla loro dignità), andando al di là del semplice "danno" o "nocumento", ed alla luce di fattori quanto più oggettivi possibili. Il Gruppo ha altresì rappresentato che la modulazione degli obblighi dei titolari in base al rischio non può mai comportare l'eliminazione assoluta di tali obblighi e che i diritti degli interessati non possono essere compressi per motivi legati al rischio "trascurabile" del trattamento, invocando il coinvolgimento delle autorità di controllo qualora l'analisi del rischio indichi un parametro elevato nonostante le misure di mitigazione adottate.

Per quanto riguarda i trasferimenti di dati personali verso Paesi terzi (capo V), il testo concordato durante la Presidenza greca (giugno 2014) mantiene l'impostazione della proposta della Commissione, che prevede un sistema gerarchico non dissimile da quello dell'attuale direttiva (adeguatezza del Paese terzo; in caso di non-adegua-

tezza, altre garanzie di natura contrattuale: clausole contrattuali *standard*, *Binding corporate rules*; altrimenti, osservanza di altri requisiti in deroga quali: consenso dell'interessato, interesse legittimo prevalente, ecc.). Da rilevare che nel capo V è stata introdotta dal Consiglio la possibilità di utilizzare codici di condotta vincolanti (per il titolare nel Paese terzo) al fine di consentire trasferimenti di dati nonché certificazioni rilasciate in base alle disposizioni del capo IV. In proposito, il Gruppo Art. 29 ha chiesto (in un proprio "*Statement*" del settembre 2014, WP 222, doc. web n. 3815204) maggiori garanzie rispetto all'utilizzo di codici di condotta (dubitando della loro effettiva vincolatività) ed al ruolo delle autorità di controllo in tale contesto.

Come si è detto, restano sul tappeto alcune questioni importanti e particolarmente controverse, sulle quali è comunque verosimile che sia possibile chiudere il negoziato entro il primo semestre del 2015, nel corso della Presidenza lettone. Si tratta di questioni sia orizzontali sia più specifiche e, quindi, relative a singole disposizioni. Fra le prime ricordiamo, innanzitutto, la necessità di delineare meglio i settori ai quali si applicherà la futura direttiva (polizia e giustizia) anziché il regolamento, disciplinando i rispettivi ambiti di competenza nella maniera più efficace e corretta possibile.

Lungamente dibattuta (e non risolta appieno) rimane anche la questione relativa agli atti delegati e di esecuzione, ossia al conferimento alla Commissione europea del potere di adottare, in maniera sistematica – e, a parere del Gruppo Art. 29, non sufficientemente giustificata – atti comunitari finalizzati a dare piena attuazione ad alcune disposizioni del regolamento; la rilevanza del tema emerge ulteriormente considerando l'impatto sui poteri di controllo dei Parlamenti nazionali alla luce del principio di sussidiarietà.

Fra le questioni più puntuali, ma di grande rilevanza, occorre menzionare quelle relative alla configurazione del "consenso" al trattamento, che secondo la proposta della Commissione deve essere (oltre che libero, informato, specifico) anche esplicito, mentre alcuni Stati membri preferirebbero mantenere la dicitura dell'attuale direttiva 95/46/CE (consenso "inequivocabile"). Sul diritto all'oblio, che è disciplinato dall'art. 17 della proposta di regolamento, i ministri hanno convenuto genericamente (durante il Consiglio GAI di ottobre 2014) di non appesantire il testo con disposizioni eccessivamente dettagliate, ma hanno sottolineato la necessità di garantire sempre il contemperamento dei diritti fondamentali in gioco (in particolare, libertà di espressione e tutela della vita privata); il dibattito è stato fortemente influenzato dalla menzionata sentenza della Corte di giustizia nel caso *Google Spain*, senza giungere però a conclusioni definite. Assai controverso anche il tema della profilazione (artt. 4 e 20 della proposta di regolamento), per la difficile individuazione di un approccio comune da adottare; si tratta di decidere se disciplinare le sole conseguenze della profilazione (come fa la direttiva 95/46/CE all'art. 15) oppure la profilazione in sé e per sé considerata, in particolare la raccolta di dati personali per tali finalità, basandosi eventualmente sull'apporto concettuale dell'analisi condotta in materia dal Consiglio d'Europa (cfr. *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*).

One stop shop

Infine, vi è il tema importante del cd. "sportello unico" (*One-Stop-Shop* - OSS) e, più in generale, dei meccanismi di collaborazione fra autorità di controllo (capi VI, VII, e VIII sulla tutela giurisdizionale). Le discussioni in sede di Consiglio GAI si sono concluse con un generale favore per il concetto di sportello unico, purché temperato con meccanismi volti ad assicurare un'effettiva "prossimità" territoriale degli interessati all'autorità competente a decidere su eventuali ricorsi. La Presidenza greca ha presentato un documento contenente alcune soluzioni volte ad introdurre i contrappesi necessari a bilanciare gli interessi in gioco e, in particolare, un ulteriore

criterio di competenza della "autorità capofila" del procedimento qualora il trattamento sia svolto a partire da un solo stabilimento di una multinazionale nell'UE ma interessi soggetti residenti in altri Stati membri. Per integrare i benefici offerti alle imprese dallo "sportello unico" con un'effettiva tutela amministrativa e giurisdizionale per i singoli interessati, si è proposto (da parte della Presidenza italiana) un meccanismo di co-decisione tra autorità locale e autorità capofila, con adozione da parte della autorità locale delle decisioni su contenziosi esclusivamente locali o di interesse solo locale (pur se in un contesto multinazionale). L'eventuale conflitto (in termini di competenza o di merito della decisione) tra due (o più) autorità verrebbe devoluto al Comitato europeo della protezione dati (EDPB), erede dell'attuale Gruppo Art. 29, al quale dovrebbe essere riconosciuto il potere di emettere decisioni vincolanti. Questa proposta ha ricevuto un sostanziale appoggio dalla maggioranza delle delegazioni; restano alcuni elementi da precisare, ma l'architettura complessiva è stata giudicata un buon compromesso fra i diversi interessi in gioco. Conviene ricordare che, in proposito, il Gruppo Art. 29 ha chiaramente indicato alcune precondizioni (*Statement* del 16 aprile 2014, doc. web n. 3815614): affermare il mantenimento della competenza territoriale delle DPA in ogni caso (anche in vista dei seguiti da dare a livello nazionale); prevedere che l'autorità capofila funga da contatto principale ma non da decisore unico; dare efficacia vincolante alle decisioni della autorità capofila nei confronti delle altre DPA coinvolte; precisare meglio la nozione di "stabilimento principale"; garantire agli interessati di poter sempre adire i giudici nazionali per impugnare le decisioni che li riguardino anche a seguito dell'intervento del meccanismo di OSS.

La proposta di direttiva

Gli incontri che si sono susseguiti in seno al Consiglio UE nel 2014 per discutere sulla proposta di direttiva hanno comportato diversi cambiamenti al testo rispetto a quello proposto inizialmente dalla Commissione. In linea generale va rilevato che, nel corso delle riunioni, molte perplessità sono state manifestate in ordine alla necessità di adottare tale nuovo strumento, essendosi diverse delegazioni espresse per il mantenimento dello *status quo* (consistente, come è noto, nella regolamentazione contenuta nella decisione quadro 977/2008) e, quindi, dei principi volti a disciplinare solo gli scambi di dati transfrontalieri (all'interno dell'Unione). È stata inoltre manifestata la necessità di definire meglio i confini rispetto alle norme che saranno contenute nel "regolamento generale" (con conseguente richiesta di inclusione nella direttiva degli aspetti legati al mantenimento dell'ordine e sicurezza pubblica) nonché di approfondire i problemi legati all'applicazione dei principi di protezioni dati all'attività giurisdizionale.

Sotto la Presidenza greca, diverse delegazioni si sono pronunciate per l'inserimento del consenso tra le basi legali dei trattamenti di dati e presentato richieste di modifica di aspetti chiave, quali il concetto di dato personale (solo i dati che portano all'identificabilità diretta), le nozioni di trattamento e di titolare/responsabile del trattamento, di profilazione: sono temi che restano pertanto tutti ancora aperti.

Nel corso della Presidenza italiana si sono tenute tre riunioni (il 29 settembre, il 27 ottobre e il 24 novembre) dedicate ad una rilettura di alcune parti dei titoli I, II e V della direttiva. Gli aspetti discussi sono stati quello del campo di applicazione (inserimento del concetto di mantenimento della sicurezza pubblica come ulteriore finalità separata da quella di prevenzione, accertamento, contrasto e repressione di reati) e quello della definizione delle autorità competenti (inserimento nella definizione anche di quei soggetti privati cui vengono delegati compiti istituzionali nelle materie coperte dalla direttiva). La Presidenza italiana ha anche proposto un nuovo testo per l'art. 8 che riguarda le condizioni di liceità per il trattamento di dati sensibili recependo le istanze di varie delegazioni che preferivano fosse mantenuto il

testo della Decisione quadro, non più basato sul binomio divieto come regola ed eccezioni ben specificate, quanto piuttosto sulla regolazione dell'uso, reso ammissibile in caso di stretta necessità.

Sul capo V della direttiva, dedicato ai trasferimenti transfrontalieri di dati, il testo presentato dalla Presidenza ha tenuto conto dell'Accordo parziale già raggiunto dal Consiglio sull'analogo capo del regolamento.

Il documento fatto circolare dalla Presidenza ha ribadito le condizioni per i trasferimenti: *in primis* l'esistenza di una decisione di adeguatezza adottata dalla Commissione europea (sentito il *Board* delle Autorità di protezione dei dati) che può essere generale (adottata secondo la procedura del Regolamento) ovvero specifica per il campo di applicazione della direttiva; in mancanza, la presenza di garanzie appropriate (clausole contrattuali o altri tipi di impegni); laddove le altre condizioni non siano presenti, la trasmissione può essere consentita in casi particolari. Il testo della Presidenza inoltre ha importato, sulla scorta dell'analogo accordo trovato sul Capo V del Regolamento, la definizione di organizzazioni internazionali.

Il testo è stato accolto favorevolmente per quanto concerne l'introduzione della definizione di organizzazioni internazionali, cui dopo una ulteriore riflessione si è deciso di aggiungere anche un riferimento ad Interpol.

Per quanto riguarda gli accordi bilaterali già in vigore che consentono gli scambi di informazioni con Paesi ed organismi terzi, sembra emergere una chiara volontà nel gruppo di mantenerne gli effetti, diversamente da quanto previsto dalla proposta di direttiva. Il Servizio giuridico del Consiglio ha fatto presente che comunque si applica il Trattato (che prevale).

La Presidenza italiana ha predisposto, al termine del suo periodo, un testo consolidato della direttiva che servirà da base per le successive discussioni sotto Presidenza lettone. In particolare il testo contiene una riformulazione dei capi esaminati sotto la Presidenza italiana (I, II e V) e alcune proposte atte a sciogliere le difficoltà delle delegazioni riguardo al campo di applicazione della direttiva ed alla definizione di autorità competenti.

23.2. *Le conferenze delle Autorità su scala internazionale*

La Conferenza internazionale delle autorità di protezione dati

La 36ª Conferenza internazionale si è tenuta a Mauritius dal 13 al 16 ottobre 2014. Le Autorità per la protezione dei dati e la *privacy* hanno esaminato, in particolare, le potenzialità e gli effetti dell'internet delle cose (*Internet of Things* - IoT). Quattro esperti, in rappresentanza del settore privato e del mondo universitario, hanno descritto alle autorità gli impatti positivi che l'internet delle cose può avere sul vissuto quotidiano, ma anche i rischi che esso comporta e i passi necessari per continuare a tutelare, anche in questo contesto, i dati personali e la vita privata.

Durante la sessione a porte chiuse, le autorità hanno adottato quattro risoluzioni ed una dichiarazione. La dichiarazione, che riguarda appunto il tema dell'*internet of things* (doc. web n. 3655156), tiene conto delle sfide che l'internet delle cose pone alle autorità di protezione dei dati e agli individui. La dichiarazione richiama tutti gli *stakeholders* a porre in essere un dibattito costruttivo sulle implicazioni delle IoT e dei *Big data* per aumentare la consapevolezza generale in ordine alle future scelte della società.

La risoluzione "*big data*" (doc. web n. 3655166) è stata fortemente voluta ed adottata al fine di sviluppare e utilizzare le tecnologie *big data* nel rispetto dei principi fondamentali di protezione dei dati, con particolare *focus* sul principio di *privacy by design*, e l'invito ad utilizzare dati anonimi per mitigare i rischi per la *privacy*. Ciò in linea con gli orientamenti espressi dal Gruppo di Berlino sul tema (v. *infra*).

La risoluzione "*Enforcement*" (doc. web n. 3655146) mira a concretizzare e rendere effettivo il quadro in cui favorire forme di coordinamento internazionali efficaci nell'attività di attuazione delle regole di protezione dati internazionalmente condivise svolta dalle autorità di controllo.

La risoluzione "*Privacy in digital age*" (doc. web n. 3655186) invita i membri della Conferenza, alla luce dello scandalo *Datagate* e del fenomeno della sorveglianza di massa, a garantire l'applicazione dei principi generali della protezione dei dati nel mondo digitale e il rispetto degli *standard* internazionali di Madrid (2009), del Patto internazionale diritti civili e politici e della Convenzione 108 del Consiglio d'Europa.

Va ricordata, infine, la risoluzione con la quale si sono accreditate le autorità per la protezione dei dati di Brema (Germania), Ghana e Senegal alla Conferenza internazionale nonché alcune organizzazioni (rispettivamente di Giappone, Bermuda, Messico, Singapore e Stati Uniti) che hanno ricevuto lo *status* di "osservatore" della Conferenza.

A margine della Conferenza si sono tenuti alcuni eventi a cui ha preso parte anche il Garante: un seminario in tema di *digital education* che si è concentrato sui criteri per garantire più efficaci politiche di sensibilizzazione sui temi *privacy* da parte delle DPA; il seminario sul Progetto PHAEDRA nel corso del quale sono stati illustrati i passi futuri per rafforzare la cooperazione internazionale nell'ambito della protezione dei dati; il seminario sull'*accountability*, organizzato dalla Nymity e la *Information Accountability Foundation*, nel corso del quale sono stati presentati i risultati dello Studio *Accountability Benchmarking* che mira ad evidenziare le modalità con cui varie organizzazioni a livello mondiale, stanno implementando il principio di *accountability*.

La Conferenza delle autorità europee (*Spring Conference*)

Come anticipato, la Conferenza di primavera dei Garanti europei, tenutasi a Strasburgo il 5 giugno 2014, si è concentrata sul tema della cooperazione europea ed internazionale nel settore della protezione dei dati e, con tre diverse sessioni, ha fatto il punto sullo stato attuale della cooperazione, sulle aspettative in merito ad essa e sulle soluzioni per il suo rafforzamento. Durante la Conferenza è stata adottata la risoluzione sulla modernizzazione della Convenzione 108 (doc. web n. 3845156) nella quale le autorità europee di protezione dati hanno messo in evidenza la necessità che tale processo di revisione, pur tenendo conto della opportunità di aprirsi a Paesi terzi, non porti in nessun modo alla riduzione dell'alto *standard* di protezione finora garantito dalla Convenzione 108.

È stata inoltre adottata la risoluzione per l'accreditamento dell'autorità di protezione dei dati della Georgia tra i membri della *Spring Conference*.

La Conferenza è stata l'occasione per ripercorrere le diverse forme di cooperazione finora attuate sia a livello europeo (*case handling*, sottogruppi del Gruppo Art. 29, ispezioni coordinate, BCR, ACC, ecc.), sia internazionale (Conferenza internazionale, GPEN, reti di autorità, cooperazione rafforzata nella nuova 108), nonché i diversi livelli di coordinamento che possono essere attuati: semplice condivisione di informazioni non riservate senza coordinamento (ad es., *case handling*), *sweep* con scambio di informazioni non riservate; scambio di informazioni riservate (ad es., GPEN); azioni coordinate e confidenziali (come nel caso dell'esame della *privacy policy* di Google). Sono stati inoltre considerati gli elementi da migliorare per una più efficace cooperazione, ed in particolare: una maggiore armonizzazione normativa, l'estensione della cooperazione anche a settori diversi dall'*enforcement*, l'approntamento di più specifiche procedure nazionali per la cooperazione, l'indicazione di diversi *contact points*, la formalizzazione delle richieste di informazione (anche per evitare la mancanza di risposte), regole più precise per la confidenzialità delle informazioni trattate, l'incremento di risorse economiche e tecnologiche per la cooperazione e l'approntamento di strutture permanenti (segretariato) per la cooperazione.

A conclusione della *Spring Conference*, è stato istituito un nuovo gruppo di lavoro – coordinato dal Consiglio d'Europa e dall'autorità di protezione dei dati francese (co-organizzatori dell'ultima *Spring*) – finalizzato all'individuazione degli strumenti europei per il rafforzamento della cooperazione in materia di protezione dei dati tra Paesi membri UE e non.

23.3. *La cooperazione tra Autorità garanti nell'UE: il Gruppo Art. 29*

L'attività delle Autorità garanti nell'UE riunite nel Gruppo Art. 29 è proseguita nel 2014 sulla base dei temi strategici generali fissati nel programma di lavoro relativo al biennio 2014-2015 adottato il 3 dicembre 2013 (doc. web n. 3815727). In particolare, il Gruppo si è impegnato, attraverso le sue riunioni plenarie (cinque nel corso dell'anno) e la costante attività dei suoi differenti sottogruppi, per assicurare un'applicazione coerente e corretta del quadro giuridico vigente e per preparare il futuro assetto giuridico, garantendo maggiore chiarezza ed efficacia nell'affrontare la globalizzazione e le sfide tecnologiche anche attraverso una più stretta cooperazione in materia di *enforcement*.

Con riferimento al nuovo quadro normativo, il Gruppo è intervenuto con proprie osservazioni, tra l'altro, in tema di "sportello unico", in materia di trasferimenti di dati in Paesi terzi – pronunciandosi a favore del mantenimento della previsione dello strumento Bcr *for processor* (strumento che risulta invece soppresso nel testo approvato in prima lettura dal Parlamento europeo) – e con riferimento all'introduzione di un approccio basato sul rischio (v., in proposito, il par. 23.1).

Il Gruppo Art. 29 e le sentenze della Corte di giustizia

Il Gruppo si è poi espresso con riferimento a due delle sentenze più rilevanti adottate in materia di protezione dei dati dalla Corte di giustizia: la citata sentenza del 14 maggio 2014, caso Google Spain (doc. web n. 3127044) e quella dell'8 aprile 2014 (C-293/12 e C-594/12), caso Digital Rights Ireland Ltd, in materia di *data retention* (doc. web n. 3845166).

In particolare, a seguito della sentenza della Corte di giustizia relativa al caso Google Spain – con cui la Corte ha riconosciuto la società statunitense come titolare del trattamento dei dati personali che appaiono nell'elenco dei risultati del suo motore di ricerca e l'applicabilità della disciplina europea (nel caso specifico spagnola) in materia di protezione dei dati, ritenendola stabilita sul territorio spagnolo alla luce delle attività, ivi svolte, di promozione e vendita degli spazi pubblicitari poi riprodotti nelle pagine dei risultati di ricerca – il Gruppo Art. 29 ha adottato un documento volto a fornire una sistematizzazione dei criteri, sia procedurali che sostanziali, per trattare le richieste di deindicizzazione dai motori di ricerca (WP 225, doc. web n. 3876849; sul punto cfr. anche par. 10.4). Le Linee guida, che riportano indicazioni ed esempi di carattere generale, potranno essere utilizzate dalle DPA per affrontare in modo quanto più omogeneo possibile i reclami/ricorsi in caso di mancata deindicizzazione, tenendo conto comunque delle peculiarità del caso di specie e sempre nell'ottica di contemperare diritto alla deindicizzazione e libertà di informazione. Il documento potrà formare oggetto di aggiornamento alla luce dell'esperienza acquisita dalle DPA.

Il Gruppo si è altresì espresso sulla sentenza dell'8 aprile 2014 (cause riunite C-293/12 e C-594/12) con la quale la Corte di giustizia ha dichiarato invalida la direttiva sulla conservazione dei dati di traffico ritenendo che dalla stessa derivi un'ingerenza di ampia portata e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati, non limitata allo stretto necessario. In particolare, con la dichiarazione del 1° agosto 2014 (doc. web n. 3815184), il Gruppo, che

guarda con favore alle conclusioni della Corte, ha incoraggiato gli Stati membri e le istituzioni comunitarie a prendere atto della sentenza che fissa specifici criteri per le normative di *data retention* e ad agire in linea con tali criteri.

Concetti-chiave della direttiva 95/46/CE

Il Gruppo ha proseguito l'attività di approfondimento di disposizioni chiave della direttiva 95/46/CE, in particolare con l'adozione del parere 6/2014 (WP 217, doc. web n. 3815154) sulla nozione di "legittimo interesse", uno dei criteri di legittimità del trattamento previsti dall'art. 7 della direttiva 95/46/CE. In tale documento il Gruppo pone il legittimo interesse (del titolare o di terzi, purché non prevalgano i diritti e le libertà fondamentali dell'interessato) tra i requisiti che legittimano il trattamento al pari delle altre basi giuridiche di cui all'art. 7 (ad es., il consenso dell'interessato). La sua applicazione non deve dunque essere residuale, solo in caso di impossibilità di avvalersi degli altri criteri previsti dalla direttiva. Al contrario, esso può risultare il criterio di legittimità più congruo – purché siano rispettati i diritti fondamentali delle persone – per evitare di fondare il trattamento su requisiti che non forniscano sufficienti salvaguardie per l'interessato (si pensi al caso del trattamento di dati in ambito lavorativo fondato sul consenso del dipendente, difficilmente "libero", considerato lo squilibrio contrattuale tra datore di lavoro e dipendente stesso). Il legittimo interesse non deve tuttavia rappresentare la facile via d'uscita per il titolare che non abbia altra base su cui fondare il trattamento. Ed infatti il parere, dopo essersi soffermato sull'analisi testuale dell'art. 7, lett. *f*), mette in luce i diversi fattori che devono essere considerati. Ad esempio, le conseguenze del trattamento sulle persone devono essere valutate secondo un'ampia accezione (non limitandosi ai soli danni materiali che potrebbero incombere sull'interessato), devono riguardare la natura dei dati, la modalità del trattamento, le ragionevoli aspettative di *privacy* della persona coinvolta, lo *status* del titolare e dell'interessato stesso. Inoltre, perché il legittimo interesse del titolare possa dirsi prevalente e quindi costituire la base giuridica del trattamento, grande attenzione va prestata alle salvaguardie ulteriori (rispetto agli obblighi fissati dalla direttiva) poste in essere dal titolare stesso (ad es., garanzie di *accountability* e trasparenza, diritto di opposizione "incondizionato", garanzia di un'immediata cancellazione dei dati, misure di sicurezza particolarmente stringenti, utilizzo di tecniche di anonimizzazione ecc.) affinché i diritti degli interessati siano adeguatamente protetti.

Il parere, che fornisce raccomandazioni in merito al futuro quadro normativo UE, è stato sottoposto a consultazione pubblica al termine della quale il Gruppo ha adottato un documento riepilogativo fornendo un sintetico riscontro alle problematiche emerse in sede di consultazione ed alcuni chiarimenti, in particolare in materia di ricerca, *direct marketing* e giornalismo (doc. web n. 3815154).

Data breach notification

Molto intensa è stata l'attività del Gruppo Art. 29 con riferimento alle sfide per la protezione dei dati sollevate dalle nuove tecnologie. In particolare, il Gruppo ha affrontato il tema della cd. *data breach notification*, l'obbligo di notifica in caso di violazione della sicurezza dei dati, previsto allo stato dalla direttiva 2002/58/CE per i soli fornitori di servizi di comunicazione elettronica ma che potrebbe essere esteso ai diversi titolari del trattamento dal nuovo Regolamento sulla protezione dei dati.

Con il parere 3/2014 (WP 213, doc. web n. 3815121), il Gruppo fornisce indicazioni ai titolari del trattamento per una corretta notifica agli interessati in caso di *data breach*, e pur riferendosi all'esistente obbligo previsto per il settore delle comunicazioni elettroniche, riporta esempi per molteplici altri ambiti, introducendo "buone pratiche" per mettere al riparo gli interessati dai rischi delle falle nella sicurezza. A differenza della notifica all'autorità competente – che deve avvenire, secondo la direttiva 2002/58/CE, per tutte le violazioni dei dati – il parere esamina le violazioni dei dati personali per le quali è richiesta anche la notifica agli interes-

sati e considera ciò che i responsabili del trattamento avrebbero potuto fare nella messa in opera dei loro sistemi per prevenire la violazione dei dati personali o, quanto meno, per individuare le misure attuabili per esentare il titolare dall'obbligo di notifica agli interessati.

Tecniche di anonimizzazione

Il Gruppo ha ultimato l'approfondimento sulle tecniche di anonimizzazione con l'adozione del parere 5/2014 (WP 216, doc. web n. 3815144) il quale esamina l'efficacia e i limiti delle tecniche esistenti rispetto al quadro giuridico dell'UE in materia di protezione dei dati e fornisce raccomandazioni per il loro impiego, tenendo conto del rischio residuo di identificazione insito in ciascuna di esse. Il Gruppo riconosce il valore potenziale dell'anonimizzazione come strategia per consentire alle persone e alla società in senso lato di fruire dei vantaggi dei "dati aperti", attenuando al contempo i rischi per le persone interessate (nella consapevolezza di quanto sia difficile creare insiemi di dati effettivamente anonimi mantenendo al contempo tutte le informazioni necessarie per espletare l'attività richiesta).

Il parere sottolinea, inoltre, che l'anonimizzazione costituisce un trattamento ulteriore dei dati personali e, in quanto tale, deve soddisfare il requisito di compatibilità con le originarie finalità del trattamento, tenendo conto delle motivazioni giuridiche e delle circostanze del trattamento successivo. Una volta resi (effettivamente) anonimi, i dati non rientrano più nell'ambito di applicazione della legislazione in materia di protezione dei dati, tuttavia le persone interessate potrebbero comunque avere diritto a forme di tutela in base ad altre disposizioni (ad es., quelle che proteggono la riservatezza delle comunicazioni).

Il parere illustra poi le principali tecniche di anonimizzazione, ossia la "randomizzazione" e la "generalizzazione". In particolare, esamina l'aggiunta del rumore statistico, le permutazioni, la *privacy* differenziale, l'aggregazione, il k-anonimato, la l-diversità e la t-vicinanza. Ne illustra i principi, i punti di forza e di debolezza, nonché gli errori e gli insuccessi comuni connessi all'impiego di ciascuna tecnica.

Internet of things

Al centro dell'attività del Gruppo è stato anche il tema dell'internet delle cose (*Internet of things* - IoT). Con il parere 8/2014 (WP 223, doc. web n. 3815214), adottato proprio in vista della discussione che si sarebbe tenuta nella Conferenza internazionale (v. par. 23.2), il Gruppo si è soffermato sui principali rischi sottesi al sempre più ampio sviluppo dell'IoT (in particolare, in associazione a *wearable computing, quantified self* e domotica), fornendo prime indicazioni su come i principi di protezione dei dati possano trovare applicazione in tale ambito. Attraverso un'ampia esemplificazione, il parere auspica anzitutto che il maggior numero di garanzie siano introdotte già nella fase progettuale e che all'utilizzatore debba rimanere il controllo dei dati trattati dall'"oggetto" in ogni fase del trattamento, anche per il tramite del suo consenso informato, libero e specifico. Alcune raccomandazioni sono rivolte a tutti gli *stakeholder* interessati (produttori, sviluppatori di app, piattaforme *social*, etc.): applicazione dei principi di *privacy by design* e *privacy by default*, redazione del *Privacy Impact Assessment* (utilizzando le indicazioni già date dal Gruppo Art. 29 nel 2011 in materia di Rfid, WP 180), minimizzazione dei dati, utilizzo di informative cd. *user-friendly*, raccolta granulare del consenso, etc.

Device fingerprinting

Nel corso dell'anno è stato anche adottato il parere 9/2014 sul cd. *device fingerprinting* (WP 224, doc. web n. 3815224), ovvero sulle tecnologie che possono essere utilizzate, in alternativa ai *cookies*, per l'identificazione univoca ed il tracciamento degli utenti dei servizi internet. Il Gruppo, in linea con precedenti prese di posizione (parere 4/2010 sull'esenzione del consenso in materia di *cookies*), ritiene applicabile l'art. 5.3 della direttiva 2002/58/CE anche al *device fingerprinting*, rendendo pertanto necessaria la previa raccolta del consenso, salvo il caso in cui l'utilizzo di tale tecnologia sia necessario per la fornitura di un servizio. Il parere sottolinea inoltre

che le disposizioni in materia di protezione dei dati personali trovano comunque applicazione ogniqualvolta si realizzi un trattamento di dati personali (come nel caso in cui la combinazione di più elementi possa portare all'identificazione dell'utente – ad es., in occasione del trattamento di un indirizzo IP).

Big data

Il Gruppo con una dichiarazione adottata il 16 settembre 2014 (WP 221, doc. web n. 3815194), si è poi espresso sul tema dei *big data* e sul loro impatto sulla protezione dei dati. In questa sede, ha sottolineato come non vi sia motivo di credere che i principi europei di protezione dei dati, come sanciti nella direttiva 95/46/CE, possano essere messi in discussione dallo sviluppo di tale fenomeno. Ha tuttavia richiamato l'attenzione sulla necessità di declinare tali principi – e in particolare quello di finalità e quello di minimizzazione dei dati – in questo nuovo contesto al fine di favorirne un'applicazione adeguata. Il tema dei *big data* è stato altresì oggetto della lettera indirizzata all'amministrazione USA in relazione al cd. Rapporto Podesta "*Big Data: Seizing Opportunities, Preserving Values*" (doc. web n. 3815624).

Google privacy policy

Grazie all'attività di cooperazione tra diverse autorità nazionali, a settembre è stata concordata dal Gruppo una lettera (doc. web n. 3815664), poi inviata a Google, relativa al *set* delle misure che la società è tenuta a rispettare affinché la propria *privacy policy* possa essere ritenuta in linea con il quadro normativo europeo in materia di protezione dei dati personali. La lettera di accompagnamento spiega che Google potrà anche adottare misure diverse da quelle indicate ove le stesse raggiungano comunque gli obiettivi richiesti (doc. web n. 3815654).

Aerei a pilotaggio remoto (RPAS)

Anche a seguito di una specifica richiesta fatta pervenire dalla Commissione europea che l'8 aprile 2014 ha adottato la Comunicazione COM(2014) 207, "Una nuova era per il trasporto aereo - Aprire il mercato del trasporto aereo all'uso civile dei sistemi aerei a pilotaggio remoto in modo sicuro e sostenibile", il Gruppo ha iniziato i lavori per predisporre un parere in materia di utilizzo degli aerei a pilotaggio remoto (cd. droni) per scopi civili (ivi comprese le attività di *law enforcement*). Il documento, che dovrebbe essere adottato entro la prima metà del 2015, fa seguito alle risposte già fornite dal Gruppo ad un precedente questionario che la Commissione aveva inviato nel 2013 (v. Relazione 2013, p. 172) e fornirà una serie di indicazioni per consentire un utilizzo di tali mezzi rispettoso dei principi di protezione dei dati. Particolare attenzione dovrà essere prestata, in particolare, ai principi di minimizzazione, necessità e proporzionalità del trattamento (soprattutto mediante l'adozione di misure di *privacy by design* e *by default* da parte, ove possibile, dei costruttori ma, soprattutto, degli operatori), al rispetto del principio di finalità e di liceità (con l'individuazione, di volta in volta, della più idonea base giuridica per il trattamento) e alle modalità per rendere edotti gli interessati.

Borders, Travel e Law Enforcement

Alla luce dei recenti scandali in materia di sorveglianza di massa, di particolare rilievo è stata l'attività svolta dal Gruppo in relazione al lavoro del *Borders, Travel and Law Enforcement subgroup*.

Parere sull'applicazione dei principi di necessità e proporzionalità nel settore del *law enforcement*

A febbraio è stato adottato il parere 1/2014 sull'applicazione dei principi di necessità e proporzionalità nel settore del *law enforcement* (WP 211, doc. web n. 3815111) anche alla luce della giurisprudenza della Corte europea dei diritti dell'uomo che, in questi anni, si è venuta consolidando in relazione all'art. 8 della Convenzione europea dei diritti dell'uomo (che stabilisce il diritto al rispetto della vita privata e familiare). Anche se i concetti di necessità (e proporzionalità) si sono sviluppati in quella giurisprudenza al di là del contesto della protezione dei dati in senso stretto, il loro rapporto con quest'ultima disciplina va tenuto in considerazione, in quanto sia la Convenzione 108 (applicabile al settore del *law enforcement*) sia la direttiva 95/46/CE, nell'introdurre restrizioni ai diritti, fanno riferimento espresso o comunque sottendono il rispetto dei criteri indicati da tale articolo.

Anche se la direttiva 95/46/CE non è applicabile in larga misura al settore dell'*ex* III pilastro, il parere sottolinea come i suoi principi sono stati estesi dai legislatori nazionali fino a coprire di regola tutti i trattamenti di dati, inclusi quelli del cd. *ex* III Pilastro, seppur con deroghe ed eccezioni. Nell'ottica del Gruppo Art. 29, anche attingendo alla giurisprudenza e all'esperienza dei membri del Gruppo, il parere ha lo scopo di indicare al legislatore e alle autorità di *law enforcement* gli elementi da tener presenti affinché le misure in materia di libertà, sicurezza e giustizia proposte per il futuro (sia in caso di introduzione di nuove misure o per modificare quelle esistenti) siano necessarie e proporzionate, invece di avere semplicemente un "valore aggiunto" o "essere utili": in particolare, sarà necessario tenere in considerazione la base giuridica, il problema specifico da risolvere (per esempio la sua gravità e il contesto sociale e culturale in cui è sorto), le motivazioni (cui sono strettamente legate le decisioni in materia di tempi di conservazione dei dati, di minimizzazione della raccolta e di qualità dei dati) e l'esistenza di elementi sufficienti a sostegno delle motivazioni che portano a scegliere quella misura.

Parere sulla sorveglianza delle comunicazioni elettroniche a fini di *intelligence* e sicurezza nazionale

Il 10 aprile 2014, il Gruppo ha adottato il parere 4/2014 sulla sorveglianza delle comunicazioni elettroniche a fini di *intelligence* e sicurezza nazionale (WP 215, doc. web n. 3815134) nel quale, alla luce dello scandalo *Datagate*, si sostiene che in nessun caso la lotta al terrorismo può giustificare forme di sorveglianza massiva e indiscriminata e si sollecitano maggiori controlli e trasparenza sulle attività dei servizi di *intelligence* unitamente all'introduzione di un quadro legale coerente ed una supervisione efficiente, anche attraverso: un effettivo coinvolgimento delle autorità di protezione dei dati; il rafforzamento degli obblighi – già gravanti sui Paesi dell'UE derivanti dalla Convenzione europea dei diritti dell'uomo e dal Trattato – di proteggere il diritto alla riservatezza ad alla tutela dei dati personali; la sollecita adozione del "pacchetto protezione dati" ed in particolare il mantenimento nella proposta di regolamento dell'art. 43a proposto dal Parlamento (obbligo di informare gli interessati ove sia stato riconosciuto ad autorità pubbliche l'accesso ai dati personali che li riguardano); l'adozione di un accordo internazionale che preveda forti garanzie per gli individui nel contesto delle attività di sorveglianza.

***Intelligence* e la sicurezza nazionale**

Al fine di sviluppare l'analisi giuridica di quanto già elaborato nel WP 215, il Gruppo ha inoltre adottato, a dicembre, un documento di lavoro sulla sorveglianza delle comunicazioni elettroniche per finalità di *intelligence* e la sicurezza nazionale (parere 18/2014, WP 228, doc. web n. 3815264). Esso contiene diverse raccomandazioni su come garantire il rispetto dei diritti fondamentali di riservatezza e protezione dei dati da parte dei servizi di *intelligence* e di sicurezza, su come migliorare la vigilanza di questi enti, pur nel rispetto della sicurezza nazionale, e ricorda a tutti i soggetti interessati la loro corresponsabilità nella progettazione e nell'applicazione di un quadro etico per la raccolta e l'uso dei dati personali nell'economia digitale. Il documento è stato presentato all'*European data governance forum* tenutosi a Parigi l'8 dicembre 2014.

Dichiarazione congiunta delle autorità di protezione dati europee in materia di sorveglianza

Sempre in tema di sorveglianza, si segnala inoltre la dichiarazione congiunta delle autorità di protezione dati europee riunite nel Gruppo Art. 29, adottata il 26 novembre (WP 227, doc. web n. 3815254). La dichiarazione (anch'essa presentata in occasione del predetto *European data governance forum* di Parigi), muovendo dalle problematiche emerse con il caso Snowden (senza limitarsi ad esse), richiama i principi fondamentali di protezione dei dati e l'importanza di un approccio preventivo fondato sulla *privacy by design* in grado di garantire un agevole esercizio dei diritti da parte degli interessati. Raccomanda inoltre una tempestiva adozione del regolamento e della Convenzione 108 modernizzata (mantenendo il più alto livello di protezione dei diritti), che gli accordi commerciali quali il TTIP e TISA non ero-

dano i principi di protezione dei dati, che una protezione rinforzata sia assicurata ai diritti dei minori, specie *online*, che la *digital education* diventi una priorità dei governi. La Dichiarazione condanna, infine, qualsiasi forma di sorveglianza massiva e indiscriminata e la conservazione non selettiva di dati.

PNR

In materia di raccolta anticipata dei dati dei passeggeri aerei (PNR), il Gruppo ha seguito inoltre lo sviluppo dei progetti nazionali che utilizzano il programma di finanziamento messo a disposizione dalla Commissione europea.

Protezione dei dati in ambito finanziario

È stata riavviata l'attività del Gruppo riguardo alle tematiche di protezione dei dati in ambito finanziario, in particolare con l'assunzione da parte del Garante del coordinamento del sottogruppo "*Financial matters*" a partire da giugno 2014, su mandato della plenaria.

L'attività del Gruppo si è concentrata sul tema dello scambio automatizzato di dati a fini fiscali, un fenomeno in crescente espansione a livello europeo e internazionale.

In particolare, anche sull'onda del consenso politico ottenuto dal FATCA (la legislazione USA anti evasione fiscale *offshore*), l'OCSE, su mandato del G20, ha adottato i cd. *common reporting standard* che si propongono quale modello globale per lo scambio di informazioni tra amministrazioni fiscali ai fini della lotta all'evasione. Il documento OCSE, oltre a prevedere criteri comuni per la raccolta (e l'invio alle amministrazioni competenti) di dati relativi ai clienti da parte degli istituti finanziari, riporta un modello di accordo che può essere utilizzato dalle amministrazioni fiscali nazionali per lo scambio di tali dati.

Il Gruppo, con la lettera indirizzata all'OCSE, al G20 e alle istituzioni comunitarie competenti, pur riconoscendo che la lotta all'evasione fiscale rappresenta un legittimo interesse pubblico, ha richiamato la necessità che tale finalità sia perseguita nel dovuto rispetto dei diritti fondamentali e non porti a raccolte e scambi massivi, non proporzionati allo scopo perseguito. La lettera fa riferimento alla sentenza della Corte di giustizia dell'8 aprile 2014 che ha invalidato la direttiva *data retention*, e sottolinea come i principi in essa contenuti abbiano portata generale e debbano essere considerati anche nel caso di scambi automatizzati di dati a fini fiscali. Richiama la necessità che gli accordi tra Stati derivanti dai CRS includano principi di protezione dei dati in maniera sostanziale e non si limitino ad un mero richiamo formale alla normativa. La lettera rinvia inoltre ad un allegato che contiene gli specifici elementi critici finora individuati nei CRS e i principi di protezione dei dati che dovrebbero essere considerati per garantire il rispetto della direttiva 95/46/CE. In particolare si segnala la necessità che gli scambi tra Stati abbiano una adeguata base giuridica, rispettino il principio di finalità (con una preliminare e chiara definizione dello scopo del trattamento ed evitando che, una volta acquisiti i dati, gli stessi siano poi impiegati per finalità incompatibili), prevedano criteri specifici di *data retention*, assicurino la trasparenza del trattamento con un'adeguata informativa agli interessati, garantiscano un agevole esercizio dei diritti, definiscano correttamente la titolarità del trattamento (e la presenza di eventuali responsabili) ed assicurino misure di sicurezza adeguate.

Il Gruppo ha continuato a seguire l'argomento dello scambio automatizzato di dati a fini fiscali anche in ragione dell'avvenuta adozione (9 dicembre 2014) della direttiva 2014/107 (recante modifica della direttiva 2011/16/UE per quanto riguarda lo scambio automatico obbligatorio di informazioni nel settore fiscale) che ha sostanzialmente recepito il modello OCSE dei CRS in ambito europeo, e in vista della predisposizione, da parte del Gruppo stesso, di future linee guida per i governi nazionali per una corretta implementazione dei principi di protezione dei dati.

Sempre sotto il coordinamento italiano, il Gruppo Art. 29 ha inoltre avviato un lavoro sul "*Multilateral Memorandum of Understanding*" (MMoU), predisposto dalla *International Organisation of Securities Commissions* (IOSCO), aperto alla firma

delle autorità di vigilanza nazionali, per una migliore cooperazione nel settore dei valori mobiliari e volto ad assicurare il rispetto delle discipline interne in tale settore. Con la lettera del 18 settembre 2014 il Gruppo si è rivolto a IOSCO, affinché in tale accordo siano tenuti in dovuta considerazione i profili di protezione dei dati (doc. web n. 3815644).

È stata altresì avviata una riflessione sull'impatto sulla protezione dei dati derivante sia dal pacchetto composto dalla direttiva 2014/65 relativa ai mercati degli strumenti finanziari (la cd. MIFID2), e dal regolamento 600/2014 (in particolare in relazione al rafforzamento previsto da tali strumenti normativi degli obblighi di registrazione di telefonate e comunicazioni elettroniche da parte delle società di investimento per consentire alle autorità competenti di svolgere i loro compiti di supervisione per un corretto andamento del mercato), sia dal regolamento 596/2014 in tema di abusi di mercato (cd. MAR).

Sia su MIFID2 che su MAR, sono stati predisposti *standard* tecnici (sottoposti a consultazione pubblica) da parte della *European Securities Markets Authority* (ESMA) con la quale il Gruppo ha aperto un dialogo al fine di orientare tali *standard* ad una corretta implementazione degli obblighi di protezione dei dati previsti dalla direttiva 95/46/CE.

Trasferimento dati all'estero

Facilitare il trasferimento dei dati all'estero salvaguardando, al contempo, il necessario rispetto del diritto alla protezione dei dati è stato, anche nel 2014, l'obiettivo che il Gruppo ha cercato di perseguire attraverso l'attività del sottogruppo *international transfers*.

***Referential* Bcr/CBPR e adeguatezza**

In quest'ottica, guardando in particolare al mondo delle multinazionali, è stato adottato a febbraio un documento di consultazione (*referential*) che individua i requisiti comuni alle norme vincolanti di impresa (Bcr) – autorizzate dalle autorità di protezione dei dati europee per i trasferimenti di dati personali effettuati, nell'ambito di un gruppo societario, al di fuori dell'Unione – e al sistema delle norme transfrontaliere in materia di *privacy* (CBPR) della Cooperazione economica Asia-Pacifico (APEC). Il documento potrà essere utilizzato, quale strumento comparativo dei due sistemi, dalle multinazionali che intendano presentare sia una domanda di approvazione di Bcr presso le DPA europee sia una richiesta di certificazione di CBPR da parte di un agente responsabile dell'APEC, al fine di ottenere una doppia certificazione (parere 2/2014, WP 212, doc. web n. 3815101).

In tema di adeguatezza delle discipline nazionali di Paesi terzi (adeguatezza in virtù della quale i trasferimenti di dati dall'UE possono avvenire senza alcun tipo di autorizzazione) e tutela dei diritti degli interessati, il Gruppo si è pronunciato con particolare chiarezza sia nel parere relativo alla (non) adeguatezza del Québec (WP 219 Opinion 7/2014, doc. web n. 3815174) che in una lettera inviata alla Commissione europea in relazione al processo di valutazione del regime attuale del *Safe Harbour* ancora in corso.

Con riferimento alla legislazione del Québec, il Gruppo ha ritenuto che la stessa, per poter essere dichiarata adeguata, necessita dell'introduzione di ulteriori misure, anche normative, volte a chiarire l'ambito di applicazione territoriale della legge nazionale, a garantire adeguata tutela ai dati sensibili (categoria non chiaramente definita dall'attuale legislazione) e individuare strumenti vincolanti per il trasferimento di dati all'estero (rilievo quest'ultimo importante tenuto conto che in Québec è stabilita l'Agenzia mondiale *anti-doping* - WADA che raccoglie e tratta i dati che gli atleti sono tenuti a comunicare per le finalità *anti-doping*, attraverso la banca dati ADAMS; cfr. al riguardo par. 4.1).

Ancor più rigorosa la lettera inviata dal Gruppo alla Commissione europea concernente il funzionamento del *Safe Harbour* (cfr. Relazione 2013, p. 181 e doc. web

n. 2983002) nella quale si sollevano dubbi in ordine all'adeguatezza del sistema come attualmente configurato e si profila la possibilità che l'accordo sia sospeso ove il processo di revisione condotto dalla Commissione con le autorità USA non porti ad un risultato positivo. La lettera fornisce diversi suggerimenti per migliorare il sistema allo stato in vigore. Si suggerisce una maggiore trasparenza in ordine ai soggetti che possono far parte del sistema, alle regole per le società che agiscono in qualità di responsabili del trattamento e una maggiore tutela dei diritti degli interessati residenti in EU (si chiede, in particolare, che agli stessi possa essere riconosciuto il diritto di adire una corte europea come pure che siano loro riconosciuti gli stessi diritti dei cittadini statunitensi). Si auspica inoltre l'introduzione di una nozione di "trattamento" analoga a quella prevista dalla direttiva, che includa anche la mera raccolta dei dati e l'inserimento di un chiaro riferimento al rispetto dei principi di necessità e proporzionalità anche nel caso in cui operi la deroga prevista per la sicurezza nazionale e sia consentita, quindi, una *disclosure* dei dati alle autorità pubbliche statunitensi (doc. web n. 3820223).

Clausole contrattuali tipo

Il Gruppo è intervenuto anche in materia di clausole contrattuali, adottando, a marzo, un documento di lavoro sul modello di clausole contrattuali *ad hoc* per i trasferimenti da un EU *processor* a non-EU *subprocessor* (WP 214, *Working document* 1/2014, doc. web n. 3815346) che potrà essere utilizzato nei casi in cui un responsabile del trattamento stabilito sul territorio europeo (EU-*processor*) intenda "subappaltare" attività che comportino il trattamento di dati a soggetti stabiliti in Paesi terzi (non EU-*subprocessor*). Le clausole, pur non essendo clausole contrattuali *standard* adottate dalla Commissione europea (come quelle previste per il trasferimento di dati da titolare a titolare e da titolare a responsabile), intendono costituire un modello cui le società possono ispirarsi nel caso di trasferimenti fra responsabili del trattamento non coperti da altri strumenti quali, ad esempio, le Bcr *for processor*. Il documento è stato aperto ad una procedura di consultazione i cui esiti dovrebbero essere resi noti nel corso del 2015.

Sempre in materia di clausole contrattuali *standard*, il Gruppo ha adottato, a novembre, un documento di lavoro (WP 226, doc. web n. 3815244) che istituisce una procedura di cooperazione per emettere pareri comuni nei casi in cui una società, con più stabilimenti in diversi Stati membri, decida di utilizzare il medesimo strumento contrattuale per i trasferimenti di dati posti in essere dalle proprie filiali stabilite in UE e si trovi, pertanto, nella condizione di doversi rivolgere alle diverse DPA competenti al fine di ottenere una valutazione circa la conformità o meno delle proprie clausole ad uno dei *set* di clausole contrattuali tipo adottati dalla Commissione (si tratta spesso di società che rendono servizi di *cloud*, come nel caso delle clausole già sottoposte da Microsoft e Amazon).

Bcr *for controller* e Bcr *for processor*

Ormai consolidata è invece la procedura per l'adozione, a livello europeo, delle regole vincolanti d'impresa (Bcr), strumento sempre più diffuso per il trasferimento dei dati effettuato tra società appartenenti ad un medesimo gruppo che operino in qualità di titolare del trattamento (Bcr *for controller*, Bcr-C) o in qualità di responsabili del trattamento (Bcr *for processor*, Bcr-P).

Nel 2014 sono state avviate 9 procedure per Bcr-C e 2 per Bcr-P e sono state concluse, con il riconoscimento dell'adeguatezza delle disposizioni nelle stesse contenute, 13 Bcr-C e 6 Bcr-P; l'Autorità è intervenuta in qualità *co-reviewer* in 5 procedure (per le autorizzazioni nazionali si fa rinvio al par. 18) fornendo specifiche indicazioni in ordine a modifiche da apportare nel testo delle Bcr (una delle quali *for processor*) proposte dalle società al fine di renderle conformi al quadro normativo europeo.

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

Europol: l'attività dell'Autorità di controllo comune (ACC)

L'attività dell'ACC Europol, che a giugno ha eletto i nuovi organi (presidente Vanna Palumbo del Garante e vicepresidente l'olandese Wilbert Tomesen), si è incentrata da un lato, come nel 2013, sull'analisi della proposta di regolamento che istituisce l'Agenzia dell'Unione europea per la cooperazione e la formazione delle autorità di contrasto (Europol) e abroga le decisioni nn. 2009/371/GAI e 2005/681/GAI del Consiglio (presentata dalla Commissione europea nel 2013, doc. web n. 2983062) e, dall'altro, sull'attività ispettiva svolta in relazione ai trattamenti di dati effettuati da Europol.

Con riguardo alle discussioni sul nuovo quadro normativo (rispetto al quale il Parlamento europeo ha adottato il proprio parere in prima lettura con emendamenti il 25 febbraio 2014) e alle modifiche proposte dal Consiglio (nell'ambito dell'approccio generale raggiunto dal Consiglio Giustizia ed Affari Interni di giugno), l'ACC ha verificato che sono stati accolti alcuni dei punti sollevati nei pareri dalla stessa resi nel 2013 (vedi Relazione 2013, p. 183), in particolare, per quanto riguarda la predisposizione di una base legale per il trattamento di dati nel sistema di messaggistica SIENA e la sua gestione e per la cooperazione diretta con le unità di analisi finanziaria (FIU) costituite in attuazione delle direttive antiriciclaggio. Passi indietro sembrano invece essere stati fatti rispetto al testo iniziale in materia di diritto di accesso degli interessati. Per quanto concerne la supervisione, una modifica importante riguarda il possibile coinvolgimento delle Autorità nazionali nel *board* accanto all'EDPS (modifica che potrà diventare definitiva però solo laddove la stessa risulti coerente con le scelte che matureranno nelle discussioni per aggiornare la base legale di Eurojust e creare l'EPPO). Alla luce di ciò, l'ACC ha adottato un terzo parere (doc. web n. 3815594) che, soffermandosi su tre aspetti principali (il trattamento dei dati sensibili e di diverse categorie di interessati, il diritto di accesso e la cooperazione tra le autorità nazionali e l'EDPS), ha concluso col ritenere il nuovo quadro normativo prospettato più fragile di quello attuale.

Per quanto concerne l'attività ispettiva, nel 2014, oltre alla tradizionale ispezione annuale di Europol svoltasi a marzo (cui ha partecipato, come negli anni scorsi, anche l'Autorità e rispetto alla quale è stato adottato a ottobre il consueto rapporto), l'ACC ha svolto, nel mese di settembre, una specifica attività volta ad accertare se le informazioni e i dati personali condivisi con Europol siano stati legittimamente acquisiti dalle autorità nazionali. L'ispezione – effettuata al fine di rispondere ad una specifica richiesta contenuta nel rapporto che la Commissione LIBE del Parlamento europeo ha adottato il 21 febbraio 2014 sui programmi di sorveglianza di massa (doc. web n. 3815717) – ha avuto ad oggetto oltre centocinquanta casi. Nella maggior parte di essi, gli elementi raccolti hanno consentito di escludere che i dati fossero stati acquisiti in violazione di legge; in alcuni casi, invece, tale verifica non ha potuto aver luogo o perché le informazioni trasmesse dalle autorità segnalanti non sono state sufficienti oppure perché coperte da un livello di classificazione che non ne consentiva la comunicazione. Alla luce di ciò, il rapporto adottato dall'ACC il 9 dicembre (doc. web n. 3815604) ha ribadito la necessità che le autorità nazionali forniscano ad Europol tutte le informazioni necessarie per consentire allo stesso di valutare la liceità delle informazioni trattate.

L'ACC ha deciso di approfondire, anche grazie all'esperienza maturata da Europol, il tema del traffico di esseri umani per definire orientamenti e raccomandazioni su come assicurare il rispetto dei principi di protezione dei dati e di tutela delle vittime nell'attività di analisi svolta da Europol e dagli Stati membri, garan-

tendo che nella fornitura di dati personali lo *status* di vittima o "potenziale" vittima sia adeguatamente evidenziato.

I sottogruppi dell'ACC hanno anch'essi continuato il loro lavoro. Il *New Project Group*, in particolare, ha approfondito alcuni nuovi progetti di Europol, riguardanti la strategia di sviluppo del sistema di messaggistica SIENA, un nuovo sistema di analisi, di archiviazione delle informazioni, il progetto per la creazione di una lista condivisa dei maggiori ricercati da parte degli Stati membri (*most wanted*).

L'ACC, al fine di instaurare/mantenere rapporti con le corrispondenti autorità dei Paesi terzi con cui Europol ha accordi operativi (che prevedono anche lo scambio di dati personali), ha incontrato, nel mese di giugno, le DPA di Svizzera, Liechtenstein, Macedonia-Fyrom e Monaco.

Il Comitato ricorsi ha ricevuto un nuovo caso da esaminare, sempre relativo ad una richiesta di riesame della risposta fornita da Europol ad una richiesta di accesso. Il Comitato, secondo quanto previsto dal regolamento interno, non avendo ricevuto le informazioni aggiuntive richieste al ricorrente, ha concluso l'analisi rigettando il ricorso.

Il Sistema Informativo Schengen: l'attività del Gruppo di coordinamento della supervisione SISII

Il Gruppo di coordinamento della supervisione SIS II, dopo il grave caso di *data breach* al SIRENE danese reso noto nel giugno 2013 (cfr. Relazione 2013, p. 185), ha proseguito la propria attività di approfondimento circa gli aspetti legati alla sicurezza del sistema, inoltrando alle autorità nazionali un questionario volto a favorire un *self-assessment* dei sistemi nazionali e della sicurezza in tema di trasmissione dei dati. Sebbene le risposte ricevute siano apparse abbastanza lacunose e disomogenee, un passo in avanti potrebbe comunque essere fatto attraverso l'entrata a regime del *Security officer network* (SON) lanciato dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (EU-LISA) proprio per il *report* di incidenti e per definire *standard* anche in relazione all'*outsourcing* di attività rilevanti nella gestione del SIS.

All'esito dei lavori avviati lo scorso anno, il Gruppo ha inoltre adottato la guida per l'esercizio dei diritti di accesso degli interessati ai dati che li riguardano contenuti nel SIS II che le autorità nazionali di protezione dei dati dovranno rendere disponibile anche nella lingua nazionale di riferimento.

Il Gruppo si è poi occupato dei criteri per l'introduzione nel sistema delle segnalazioni concernenti i veicoli rubati e delle ricerche sistematiche nel SIS sui clienti degli alberghi. La discussione in corso è spinta da alcuni Paesi che premono perché, con riferimento al tema dei veicoli rubati, l'interpretazione della relativa norma contenuta nella decisione SIS II sia tale da poter obbligare la cancellazione dal SIS delle segnalazioni nel momento in cui l'oggetto segnalato sia stato ritrovato o la condotta richiesta si sia perfezionata.

In tema di verifiche sistematiche del SIS sui clienti degli alberghi, il Gruppo ha ritenuto che, non avendo il nuovo quadro legale inciso sul contenuto della previgente normativa, restasse del tutto confermato il parere espresso nel 2011 dall'ACC Schengen che riteneva tale verifica non rispettosa del principio di finalità.

Gruppo di supervisione Eurodac

Nel corso delle riunioni tenutesi nel 2014, il Gruppo di supervisione del sistema Eurodac, partendo dall'approvazione del regolamento interno e della relazione di attività del biennio 2012-2013, ha analizzato gli aspetti su cui prioritariamente intervenire prima dell'entrata in vigore della nuova base giuridica (il 20 luglio 2015) derivante dall'adozione, il 26 giugno 2013, della proposta di rifusione (cd. *recast*) del regolamento Eurodac (regolamento (UE) n. 603/2013: cfr. Relazione 2013, p. 186, doc. web n. 2983052).

Il Gruppo ha deciso di impegnarsi, da un lato, a verificare la congruità ed esattezza degli elenchi delle autorità nazionali che possono accedere al sistema e la qualità delle impronte e, dall'altro, in previsione dell'entrata in vigore del nuovo quadro

giuridico, a verificare il funzionamento del sistema sia a livello di unità centrale (trasferita da Lussemburgo a Strasburgo e gestita dall'Agenzia europea per la gestione operativa dei sistemi IT su larga scala, EU-LISA) che a livello nazionale. La verifica dovrà approfondire, in particolare, le nuove funzionalità e le modifiche introdotte nel sistema per consentire l'accesso da parte delle autorità di *law enforcement* come ora previsto dal Regolamento (cfr. al riguardo Relazione 2013, p. 186), la cancellazione anticipata dei dati, i ruoli e le responsabilità dei diversi soggetti abilitati ad accedere ed inserire dati nel sistema, la trasmissione di dati a Paesi terzi, il cd. *blocking/marking* dei dati, le misure di sicurezza e l'esercizio dei diritti dell'interessato.

L'attività di verifica si svolgerà probabilmente in sinergia con gli altri due gruppi di supervisione (VIS, SIS II) gestiti da EU-LISA, tenuto conto della struttura informatica comune ai tre sistemi, realizzata sulla base del principio di interoperabilità delle piattaforme.

Il Sistema Informativo Visti [VIS]: Gruppo di coordinamento della supervisione

La qualità delle impronte raccolte è tra i temi trattati dal Gruppo di coordinamento della supervisione VIS considerata l'assenza di *best practices*, in particolare per la raccolta delle impronte biometriche (impronte digitali), spesso effettuata, attraverso contratti di *outsourcing*, da fornitori di servizi stabiliti in Paesi terzi. A tal proposito, sulla scorta di un approfondimento circa gli aspetti legali e le condizioni contenute nell'art. 43 del Regolamento (CE) n. 810/2009 del 13 luglio 2009 che istituisce il codice comunitario dei visti, il Gruppo ha predisposto una nota in cui evidenzia gli aspetti di protezione dati rilevanti, soffermandosi anche sull'eventuale possibilità per le autorità di protezione dei dati di effettuare controlli sull'operato di tali società all'estero. La nota si aggiunge ad una richiesta formulata alle DPA nazionali volta a prevedere controlli nei consolati per verificare *in loco* sia le modalità di raccolta delle informazioni (dal punto di vista delle misure di sicurezza adottate e delle regole che le società esterne devono rispettare con riferimento alla raccolta, al trattamento e alla restituzione dei dati) sia l'osservanza degli obblighi in materia di protezione dei dati; ciò, in particolare, per quanto riguarda l'informativa resa ai richiedenti il visto in relazione al possibile esercizio dei diritti di accesso, rettifica, etc. (soprattutto in caso di diniego del visto in presenza di una segnalazione Schengen). Un altro aspetto delicato su cui il Gruppo si è soffermato, ha riguardato alcuni casi di non allineamento VIS e SIS e quindi l'uso di informazioni SIS non aggiornate, con conseguenti effetti sull'accettazione/rifiuto del visto.

Sono stati inoltre definiti tre questionari (rispettivamente relativi a: lista delle autorità che possono accedere al VIS; accesso al VIS da parte delle autorità di *law enforcement* in base alla decisione 2008/633/GAI; esercizio dei diritti degli interessati) che consentiranno alle DPA di valutare eventuali carenze rispetto a quanto previsto dalle norme di riferimento; sulla base degli esiti di tali questionari, il Gruppo potrà decidere di intervenire adottando specifiche raccomandazioni laddove necessario.

Sono infine proseguiti i lavori per la definizione di una sorta di documento di metodologia comune per lo svolgimento delle ispezioni o *audit*.

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 SID si sono riunite *back to back* condividendo la supervisione sullo stesso *database*, dove sono contenuti dati relativi ad operazioni che possono anche coinvolgere fattispecie criminali. Il *database* peraltro risulta poco popolato e scarsamente utilizzato. Proprio per rimarcare il desiderio di procedere in parallelo nell'attività di supervisione che sostanzialmente riguarda gli stessi *file*, il Gruppo di supervisione ha eletto come vice *chair*, il *chair* dell'ACC Dogane.

Circa le attività, l'ACC Dogane ha fatto progressi per la definizione di un questionario, da inviare ad OLAF ed alle stesse DPA, come *follow up* dell'ispezione svoltasi nel 2011.

Per quanto concerne il Gruppo di supervisione, è stato discusso il programma di lavoro per il 2014-2015, che, una volta adottato, sarà comunicato all'esterno, in particolare a Commissione, Consiglio, Parlamento europeo.

Il Gruppo ha deciso, sulla scorta di quanto già fatto dalle altre autorità di supervisione, di lavorare su una guida per l'esercizio del diritto di accesso al sistema.

23.5. *La partecipazione ad altri comitati e gruppi di lavoro internazionali*

Consiglio d'Europa: CAHDATA

Anche il 2014 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, volto ad adeguarne i principi al mutato scenario tecnologico e ad assicurare un alto livello di tutela del diritto alla protezione dei dati. In particolare, si sono svolte la seconda e la terza (ed ultima) riunione (rispettivamente il 28-30 aprile e il 1-3 dicembre) del sopra menzionato CAHDATA (vedi par. 23).

Nell'ultima riunione del suo mandato, il CAHDATA, il cui rappresentante per l'Italia è il segretario generale del Garante Giuseppe Busia, ha adottato il testo finale della Convenzione modernizzata (doc. web n. 3815674). Tuttavia, seppur conclusosi con l'approvazione del testo, il processo di modernizzazione è stato fortemente influenzato dal parallelo lavoro di riforma del quadro di regole in materia di protezione dei dati in atto in ambito UE. La Commissione europea, che ha partecipato ai lavori del CAHDATA sulla base di un mandato del Consiglio UE a negoziare per conto degli Stati UE nelle materie di competenze comunitaria, non avendo (come si è anticipato) ancora sciolto alcuni nodi in sede di discussione del nuovo regolamento UE sulla protezione dei dati, pur dando un generale supporto al testo del CAHDATA, ha mantenuto riserva su alcuni principi (v. *infra*). Sul testo adottato dal CAHDATA, accanto ad alcune riserve di delegazioni nazionali, permangono quelle della Commissione che potranno venir meno solo una volta raggiunto un accordo tra gli Stati nell'elaborazione del Regolamento UE.

Il CAHDATA ha comunque dato mandato al segretariato del Consiglio d'Europa di predisporre il protocollo emendativo della Convenzione 108 che rifletterà il testo concordato in riunione e di allineare il *memorandum* esplicativo, nel frattempo predisposto dal Comitato T-PD, a quanto deciso in riunione. Il testo della nuova Convenzione 108 – che darà conto in nota delle riserve – sarà trasmesso al Comitato dei ministri del Consiglio d'Europa nel corso del 2015, passo comunque necessario per la finalizzazione della nuova Convenzione in sede di CoE.

T-PD

Sempre nell'ambito del Consiglio d'Europa è proseguita l'attività del T-PD, Comitato consultivo della Convenzione 108/1981 a cui il Garante partecipa da anni, anche nella sua composizione ristretta (T-PD *bureau*) e con l'incarico, ottenuto nel 2014, della vice-Presidenza.

Il T-PD, che nel 2012 aveva concluso il lavoro tecnico relativo alla modernizzazione della Convenzione 108, con l'adozione del un documento finale contenente le proposte di revisione (poi impiegato dal CAHDATA come base di discussione), ha proseguito il suo lavoro di approfondimento e supporto per la modernizzazione della 108, in particolare con la predisposizione del *memorandum* esplicativo che accompagnerà la nuova Convenzione.

È giunto invece a conclusione il lavoro del T-PD sul processo di revisione della raccomandazione 89(2) sulla protezione dei dati in ambito lavorativo. Nella plenaria di giugno il T-PD ha infatti adottato la nuova bozza di raccomandazione volta a sostituire il testo del 1989, adottata infine dal Comitato dei ministri il 1° aprile

2015 [v. Recommendation CM/Rec(2015)5]. La raccomandazione modernizzata, che riflette le nuove sfide per la protezione dei dati intervenute in ambito lavorativo (determinate *in primis* dalla crescente globalizzazione e dall'impiego di nuove tecnologie), mira ad attualizzare i principi già contenuti nella raccomandazione (89)2. Essa introduce specifiche garanzie volte ad evitare il controllo ingiustificato su impiego di *e-mail* e internet da parte del dipendente, il divieto di introdurre dispositivi che abbiano come scopo quello di monitorare l'attività del dipendente, nonché garanzie sull'impiego di dispositivi biometrici e sistemi che consentano la localizzazione del lavoratore.

La necessità di attualizzare i principi di protezione dei dati si è avvertita anche con riferimento alla raccomandazione (97) 5 sui dati sanitari, su cui pure ha continuato a lavorare il T-PD.

In particolare è stato predisposto un questionario, trasmesso nel corso dell'anno ai soggetti competenti a livello nazionale (autorità di protezione dei dati, ministeri della salute, erogatori di servizi sanitari e associazioni di medici e di pazienti), volto a verificare il livello di implementazione della raccomandazione, nonché a fotografare lo stato dell'arte in merito all'impiego di nuove tecnologie in ambito sanitario e al loro impatto sulla protezione dei dati, in particolare con riferimento ai fascicoli sanitari elettronici, alle *app* mediche, all'uso di Rfid e alla diffusione di tecniche di profilazione.

È proseguita la riflessione sull'esigenza di rafforzare e aggiornare i principi di protezione dei dati anche con riferimento al settore della polizia, allo stato contenuti nella raccomandazione (87)15. Il processo di modernizzazione di tali principi non comporterà tuttavia una revisione di tale Raccomandazione che appare ancora valida nei suoi principi generali.

Piuttosto, il *bureau* del T-PD ha concordato riguardo all'opportunità di lavorare ad un progetto di linee guida per gli operatori del settore, volte a dare più concreta applicazione ai principi della (87)15.

Il T-PD è stato anche coinvolto, insieme al Comitato del Consiglio d'Europa sul *cybercrime* (T-CY), l'EDPS e il Gruppo Art. 29, nella riflessione sul progetto di protocollo addizionale alla Convenzione *cybercrime* riguardo all'accesso da remoto ai dati situati in Paesi terzi e nel *cloud* nonché all'accesso transfrontaliero ai dati in possesso dei *provider* di servizi di comunicazione elettronica da parte di Paesi terzi, che presenta aspetti problematici per il suo impatto sulla protezione dei dati e sui principi della Convenzione 108 (v. lettera congiunta del Gruppo Art. 29 e T-PD del 28 novembre 2014, doc. web n. 3816035).

È apparsa evidente, anche in questo caso, la necessità che siano messe in atto strategie per rispondere alle nuove sfide emerse negli ultimi anni, in particolare alla luce delle rivelazioni di Snowden, e che, pertanto, il Consiglio d'Europa debba promuovere l'adesione da parte degli Stati alla Convenzione *cybercrime* e la parallela adesione alla Convenzione 108.

Il T-PD ha, per la prima volta, affrontato il tema delle implicazioni sulla protezione dei dati provenienti dagli scambi automatizzati di dati tra Stati in relazione alla lotta all'evasione fiscale, al riciclaggio, al finanziamento del terrorismo e alla corruzione. La riflessione è sorta con particolare riferimento agli "*Standard for automatic exchange of financial account information*" dell'OCSE (cd. "*Common Reporting Standard* – CRS, oggetto, come si è visto, di intervento del Gruppo Art. 29 (v. par. 23.3).

Tenuto conto dello scarso rilievo dato alla protezione dei dati nell'ambito dei CRS, nella plenaria di giugno, il T-PD ha adottato un parere volto a richiamare l'attenzione sulla necessità che tali scambi siano effettuati nel pieno rispetto dei principi della Convenzione 108 (doc. web n. 3815737).

È stato inoltre adottato un parere del T-PD sulla raccomandazione 2041(2014) dell'Assemblea parlamentare del Consiglio d'Europa sulla protezione dell'utente e la sicurezza nel *cyberspazio* (doc. web n. 3815747).

Il T-PD *bureau* ha poi adottato due pareri, rispettivamente, sulla bozza di Raccomandazione sull'uso di dati sanitari, in particolare genetici, a fini assicurativi (doc. web n. 3815757), e sul documento di lavoro sulla ricerca su materiali biologici di origine umana (doc. web n. 3876829), entrambi sottoposti al T-PD dal Comitato di bioetica del Consiglio d'Europa con il quale è stato aperto un dialogo (anche attraverso incontri *back to back* dei rispettivi *bureau*) su temi di interesse comune.

È stata infine avviata una riflessione sul tema *big data* che sarà oggetto di maggiori approfondimenti nel 2015, probabilmente anche attraverso la predisposizione di un rapporto che esamini le diverse problematiche emerse in tale settore con riferimento alla protezione dei dati finora, e valuti la necessità di declinare i principi *privacy* al fine di assicurare una adeguata protezione dei diritti fondamentali delle persone.

OCSE

In ambito OCSE l'Autorità ha continuato a partecipare ai lavori del SPDE (*Working Party on Security and Privacy in Digital Economy*) – il cui lavoro si è concentrato sulla revisione delle Linee guida Sicurezza OCSE del 2002 (*Recommendation Concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*) – ed anche per il 2015 è stata riconfermata nel *bureau* del Gruppo. Quest'ultimo ha compiuto progressi nel processo di revisione e si è riunito più volte in sessioni di redazione informali in cui si sono discusse le varie versioni (sino alla quinta) della bozza della raccomandazione rivista. La discussione è stata molto lunga ed ha tenuto conto degli *input* forniti dalle diverse delegazioni nel corso dell'anno, con un complessivo miglioramento di tutte le sezioni della bozza di raccomandazione. La sezione relativa alla strategia nazionale è stata anche essa rivista. Di grande impatto l'affermazione contenuta nella quinta versione del testo, per la quale la raccomandazione rappresenta una solida base per attuare il principio di "salvaguardia di sicurezza" delle *privacy guidelines* dell'OCSE. Il Gruppo ha anche elaborato una prima bozza di "*Companion Document*" delle *OECD Security Guidelines.* Si tratta di un *work in progress* che segue lo sviluppo della raccomandazione stessa, quale documento di accompagnamento/supporto/spiegazione di gran parte del contenuto della bozza di raccomandazione rivista.

L'attività del SPDE si è inoltre concentrata sull'esigenza di implementare le linee guida *privacy*, adottate nel 2013 (v. Relazione 2013, p. 189) 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.

Il Gruppo ha altresì discusso il progetto CSIRTs (e relativi progressi del documento di riferimento) che mira a migliorare la comparazione internazionale tra dei prodotti statistici (CSIRTs). La discussione è proseguita in un apposito incontro che si è tenuto l'11 dicembre 2014 in vista della definizione dei prossimi passi per il lavoro sugli strumenti per misurare il rischio di *cybersecurity.* L'incontro si è basato sul documento *Improving the International Comparability of Statistics Produced by Computer Security Incident Response Teams: Statistical Guidance* che descrive il progetto, gli indicatori statistici individuati e che verranno prodotti dai CSIRTs per un futuro confronto nonché l'esito di uno studio di fattibilità su cui tarare meglio l'obiettivo. Si ricorda che i CSIRTs sono stati categorizzati distinguendo tra capacità, incidenti, condizioni di rischio, impatti e consapevolezza tecnica degli strumenti stessi. Il Gruppo ha manifestato l'intenzione di continuare a coinvolgere la comu-

nità CSIRT nello sviluppo di linee guida statistiche o di un manuale per i CSIRTs finalizzato a garantire la qualità e la comparabilità internazionale.

Un altro settore al quale lo SPDE ha dedicato attenzione è quello relativo al valore economico dei dati e al loro ruolo nel promuovere la crescita economica e il benessere globale, con particolare riferimento ai cambiamenti tecnologici e organizzativi rappresentati dai *big data*. Lo SPDE ha confermato l'intento di studiare come la raccolta, l'analisi e l'uso di sempre più grandi flussi di dati digitali possono generare aumenti di produttività, promuovere l'innovazione e migliorare l'efficienza, in particolare in settori quali la sanità, la scienza e la fornitura di servizi pubblici. Inoltre, il Gruppo ha condiviso la necessità di continuare ad analizzare le implicazioni politiche della *data driven economy* in settori quali la *privacy* e la tutela dei consumatori, lo sviluppo delle competenze, l'occupazione e la concorrenza. Il Gruppo ha messo in evidenza come il settore dei *big data*, secondo le previsioni, avrebbe un potenziale di crescita di 16,9 miliardi di dollari entro il 2015.

Privacy Risk Framework Project

Nell'ambito del nuovo progetto del *Centre for Information Policy Leadership Hunton & Williams*, il *Privacy Risk framework Project*, dedicato all'approccio basato sulla valutazione dei rischi (cd. *risk-based approach*) che il trattamento dei dati personali può comportare da parte dei titolari del trattamento, si sono tenuti due *workshop* (il 20 marzo e il 18 novembre 2014) – cui hanno partecipato anche esperti dell'*Accountability project* (in merito al quale v. Relazione 2013, p. 190) – incentrati sulla catalogazione dei diversi tipi di rischi e danni alla *privacy*, sugli strumenti da sviluppare per trasformare detto approccio in azioni concrete, sugli strumenti di valutazione del "rischio *privacy*" e sulle relative implicazioni.

Nell'ultimo documento elaborato dal Centro ed oggetto di discussione del secondo *workshop* "*Paper Two of the Project on Privacy Risk Framework and Risk-based Approach to Privacy*", sono stati più approfonditamente affrontati il ruolo della valutazione e gestione dei rischi in materia di protezione dei dati come recepite in diverse norme di legge ed interpretate dalle autorità di protezione dei dati e le modalità di attuazione pratica da parte delle organizzazioni cosiddette *accountable*. È stato inoltre dibattuto il ruolo delle stesse autorità di protezione dei dati e la possibilità di porre in essere una "prioritarizzazione" delle segnalazioni e ricorsi relativi a trattamenti dei dati personali pericolosi in base al livello di rischio paventato. Il confronto tra regolatori e imprese ha anche focalizzato l'attenzione degli esperti sullo stato dell'arte della norma relativa al *RBA* nel Regolamento europeo sulla protezione dati in corso di adozione. In particolare sono stati illustrati gli sforzi della Presidenza italiana su tale norma, evidenziando che l'adozione di un *risk-based approach*, che calibri gli obblighi del titolare del trattamento sul rischio che comporta il trattamento stesso, è già stata condivisa dall'Italia nel corso dei consigli GAI di marzo e di giugno 2013.

IWGDPT

L'Autorità ha proseguito la sua partecipazione all'*International Working Group on Data Protection in Telecommunication* (IWGDPT, cd. Gruppo di Berlino) che si è riunito il 5-6 maggio a Skopje e il 14-15 ottobre 2014 a Berlino.

La riflessione già avviata sul tema *big data* ha portato all'adozione di un documento di lavoro (ripreso dalla risoluzione della Conferenza internazionale delle autorità di protezione dei dati: v. par. 23.2) che, rivolgendosi a soggetti istituzionali, industria e società civile, mira a identificare le principali sfide per la protezione dei dati che derivano dalla crescita esponenziale di tale fenomeno e a fornire raccomandazioni sull'applicazione dei principi di protezione dei dati in tale settore (doc. web n. 3815684). L'impiego dei cd. *big data* solleva più criticità per la protezione dei dati, in particolare per il principio di minimizzazione dei dati e il principio di finalità. Inoltre, l'utilizzo dei *big data* appare connotato da una marcata opacità che impedisce all'interessato di esercitare un controllo sui dati a sé riferiti; presenta forti

rischi di re-identificazione attraverso l'incrocio di informazioni derivanti da diverse fonti e di scarsa precisione nell'attribuzione di profili agli individui coinvolti (sui quali possono ricadere conseguenze significative). Inoltre, il fenomeno *big data* si fonda sull'impiego di algoritmi che non sono necessariamente neutrali ma riflettono specifiche scelte (con il conseguente rischio di stereotipizzazione e discriminazione delle persone). Per queste ragioni il Gruppo ha evidenziato l'urgenza di mantenere alto il livello di tutela dei dati al fine di salvaguardare le condizioni per una società fondata sul rispetto dei diritti e delle libertà fondamentali.

Così, i principi di protezione dei dati – in particolare la valorizzazione del consenso dell'interessato (specie con riferimento trattamenti con finalità di profilazione), procedure robuste di anonimizzazione dei dati, maggiore trasparenza, attività di sensibilizzazione riguardo all'impatto di *big data* su diritti fondamentali e l'impiego di tecniche di *privacy by design* – costituiscono elementi imprescindibili per una gestione corretta dei *big data*, conciliando in questo modo i benefici dei *big data* con la tutela delle persone.

Nel corso dell'anno il Gruppo ha portato a termine anche il lavoro di approfondimento sul tema "*own devices*", ossia di quei dispositivi individuali (quali *tablet* e *smartphones*) condivisi all'interno di una rete (in diversi contesti: all'interno di una pubblica amministrazione, un contesto lavorativo, un esercizio commerciale, ecc.). Nella riunione di Berlino, il Gruppo ha adottato uno specifico parere sui rischi per la *privacy* e la sicurezza derivanti dall'impiego di tali dispositivi (doc. web n. 3815694).

A fronte del crescente impiego del cd. BYOD (*bring your own device*) in diverse realtà lavorative, il Gruppo ha fornito specifiche raccomandazioni alle organizzazioni che intendano avvalersene per minimizzarne le ripercussioni sulla riservatezza individuale, a cominciare dalla necessità di svolgere una valutazione di impatto del BYOD che tenga conto, tra l'altro, della reale esigenza di ricorrere a tali dispositivi (specie nel caso in cui possano essere trattati dati sensibili), dei rischi di falle nella sicurezza dei dati e delle conseguenze sulla reputazione delle persone in caso di perdita dei dati. Il parere si sofferma anche sull'opportunità che le organizzazioni: forniscano specifiche *policy* volte ad identificare gli obblighi dei dipendenti in relazioni all'uso di "*own device*"; assicurino l'adeguato supporto per gli utilizzatori; definiscano adeguate politiche di sicurezza che mettano l'impiego dei dispositivi da parte dei dipendenti al riparo da interferenze nella loro vita privata.

Data retention – Expert Group

È proseguita la partecipazione dell'Autorità nel *data retention expert group*, gruppo di esperti istituito dalla Commissione europea con l'incarico di approfondire gli aspetti legati alla direttiva 2006/24/CE (cd. *data retention*) per la redazione di una sorta di manuale delle buone prassi per guidare l'attività delle autorità nazionali competenti. L'attività è stata però interrotta a seguito della sentenza della Corte di giustizia dell'8 aprile 2014 (v. par. 23.3), non essendo più nelle competenze della Commissione l'individuazione di modalità di recepimento della direttiva ormai invalidata dalla Corte.

Cooperazione internazionale IECWG, GPEN, PHAEDRA *project*

Si è ulteriormente intensificata l'attività dei Gruppi di lavoro dedicati al coordinamento delle attività internazionali di *enforcement*, anche alla luce di quanto richiesto dalla risoluzione sull'*enforcement* adottata nella 36ª Conferenza internazionale delle autorità di protezione dati (v. par. 23.2) e dal lavoro del Gruppo di coordinamento delle attività internazionali di *enforcement* (IECWG) sfociato nella redazione di un Accordo (*Arrangement*) di cooperazione internazionale di *enforcement*, adottato nel corso della medesima Conferenza.

GPEN

In tale scenario, si è ulteriormente rafforzata (anche attraverso numerose *conference call*) l'attività del *Global Privacy Enforcement Network-GPEN*, la prima rete internazionale di cooperazione transfrontaliera in tema di *enforcement* (lanciata nel

2010). Su *input* del GPEN, il Garante (membro del Gruppo) ha svolto il 13 e 14 maggio 2014 lo *Sweep* su alcune applicazioni mediche scaricabili su *smartphone* e *tablet* per verificare il grado di trasparenza sull'uso delle informazioni degli utenti, le autorizzazioni loro richieste per scaricare le applicazioni e il rispetto della normativa italiana sulla protezione dati. Sei funzionari dell'Autorità hanno analizzato, tramite due *devices*, 16 *app* mediche individuate tra le 50 *Top App* che il coordinatore centrale dello *Sweep* ha fornito. I risultati dello *Sweep* sono stati poi resi pubblici con una lettera congiunta delle Autorità che hanno partecipato all'iniziativa (doc. web n. 3602403), indirizzata alle maggiori piattaforme e operatori del mercato delle app (quali Apple, Google, Samsung, BlackBerry, Microsoft, Amazon, LG, Firefox, e Nokia), in cui si è evidenziato che ci sono stati numerosi casi di App prive di qualsiasi *privacy policy* (o altre informazioni sulla *privacy*).

PHAEDRA *project*

È proseguita l'attività del PHAEDRA *project*, progetto europeo (supportato dal Garante) volto a sostenere una migliore cooperazione e il coordinamento tra i Commissari *privacy* e le autorità di protezione dei dati di tutto il mondo, come messo in luce anche nel seminario tenutosi nel corso della 36ª Conferenza Internazionale delle autorità di protezione dati (v. par. 23.2) nonché nel corso della conferenza tenutasi a Cracovia presso l'autorità polacca dedicata a "*Come rafforzare la privacy: lezioni di attuali implementazioni e prospettive per il futuro*".

XXVI *Case Handling Workshop*

Si è tenuto a Skopje il 6 e 7 ottobre il *XXVI Case Handling Workshop*, incontro annuale che consente alle autorità di protezione dei dati europee e non di confrontarsi su temi di attualità. La discussione si è concentrata sulla casistica delle autorità in relazione al *marketing* indesiderato, al trattamento di dati biometrici, alla videosorveglianza (in particolare sull'utilizzo di *dashcam*). Una sessione, dedicata ai trasferimenti di dati all'estero, ha consentito uno scambio di opinioni in ordine a due aspetti rilevanti ma non ancora pienamente affrontati dalle DPA: il trasferimento di dati personali tra autorità pubbliche e il trasferimento di dati verso gli Stati Uniti (dal quale è emerso uno scarso utilizzo degli strumenti di tutela indicati nel *Safe Harbour).*

Cooperazione con altre Autorità

L'Autorità ha continuato a partecipare a programmi di partenariato europeo negli ambiti di competenza, 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 del Progetto TAIEX della Commissione europea, il 1° luglio si è svolto a Skopje un *Workshop* su *Privacy by Design, Privacy Impact Assessment* e *Privacy-enhancing technologies* volto a favorire il corretto utilizzo di tali strumenti da parte dei titolari del trattamento. Il 10 e l'11 novembre si è inoltre tenuto presso la sede dell'Autorità un incontro con una delegazione macedone con lo scopo di illustrare le attività poste in essere dal Garante in materia di *cookies* e in ambito ispettivo.

È inoltre proseguita l'attività di cooperazione con l'autorità di protezione dei dati albanese che, in vista di un accordo programmato per il 2015, si è incentrata sull'obiettivo di assicurare la tutela dei dati personali raccolti e utilizzati da soggetti pubblici e privati che operano in Albania (dove negli ultimi anni molte aziende italiane hanno spostato i centri di assistenza ai clienti).

È parimenti proseguita la cooperazione con l'Agenzia statale per la protezione dei dati personali della Repubblica del Kosovo volta a promuovere lo scambio di informazioni e di esperienze con il Garante, con l'intento di assicurare un'applicazione il più possibile uniforme della legislazione in materia di trattamento di dati personali.

24 Comunicazione, trasparenza, ricerca e documentazione

24.1. *La comunicazione del Garante: profili generali*

Già da qualche anno l'Autorità ha rinnovato le strategie di comunicazione per raggiungere in modo efficace anche il mondo dei cd. nativi digitali sperimentando nuovi canali, nuove tecniche e nuovi prodotti comunicativi ritenuti più idonei a stimolare i giovani utenti ad un uso consapevole della rete, in particolare, dei *social network*. Ciò al fine di attuare al meglio uno dei propri compiti istituzionali, quello di promuovere e sviluppare nella società italiana la consapevolezza del diritto alla protezione dei dati personali e del ruolo svolto al riguardo dall'Autorità (cfr. i dati di sintesi riferiti al 2014 nella sez. IV, tab. 2).

Particolarmente attento a quanto accade anche nello "spazio digitale", il Garante ha focalizzato il proprio impegno su alcuni grandi temi (più ampiamente trattati nell'ambito della Relazione): il diritto all'oblio, i *social network* e l'allarme destato dal cyberbullismo e dall'*hate speech*; il *cybercrime* e il furto d'identità; le tecniche di tracciamento e la profilazione degli utenti *online*; l'internet delle cose e le tecnologie indossabili; i grandi monopoli della rete; le *app*, in particolare quelle mediche; il *dossier* sanitario elettronico e l'utilizzo dei dati dei pazienti; la trasparenza della p.a. *online* e le garanzie da assicurare ai cittadini; le nuove regole per i pagamenti con *smartphone* e *tablet* (*mobile payment*); il corretto rapporto tra diritto di cronaca e riservatezza delle persone, in special modo se minori, sui *media* e sul web.

Significativa anche l'informazione sugli aspetti più legati alla "dimensione fisica" delle persone: il *telemarketing* aggressivo; le telefonate mute; il fisco e la lotta all'evasione; la tutela dei lavoratori; il mondo della scuola; i sistemi di videosorveglianza; l'utilizzo dei sistemi biometrici e la firma grafometrica; l'uso dei dati dei cittadini da parte di partiti e movimenti politici; le ricette in farmacia.

Le questioni sopra ricordate e l'attività del Garante hanno trovato largo spazio e attenzione sui *media*, ed in special modo sulle testate *online* ed i *blog*. Il Servizio relazioni con i mezzi di informazione ha selezionato oltre 52.000 articoli di interesse dell'Autorità. Sulla base della rassegna stampa elaborata quotidianamente, le pagine dei maggiori quotidiani e periodici nazionali, dei principali quotidiani locali e dei media *online* che hanno trattato i temi legati alla *privacy* sono state 12.500, delle quali 3.700 dedicate esclusivamente all'attività del Garante. Le prime pagine sono state oltre 650 (di cui 170 riguardanti la sola Autorità). Le interviste, gli interventi e le dichiarazioni del presidente e dei componenti dell'Autorità pubblicate e riprese sulla carta stampata sono state complessivamente 177 (e 222 *online*); andate in onda su tv e radio nazionali e locali 37; le citazioni relative all'attività del Garante in programmi televisivi e radiofonici nazionali circa 400.

24.2. *L'Autorità trasparente*

L'articolo 24-*bis*, d.l. 24 giugno 2014, n. 90, convertito, con modificazioni, dalla l. 11 agosto 2014, n. 114, ha integralmente sostituito l'art. 11, d.lgs. n. 33/2013 in materia di "Riordino della disciplina riguardante gli obblighi di pubbli-

cità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" introducendo un nuovo "ambito soggettivo di applicazione" che ricomprende tra le "pubbliche amministrazioni" alle quali la disciplina di trasparenza si applica, ora, "integralmente" anche le autorità amministrative indipendenti di garanzia, vigilanza e regolazione. A decorrere dal 19 agosto 2014, pertanto, è venuta meno la possibilità per le Autorità indipendenti di dare attuazione alla normativa in materia di trasparenza "secondo le disposizioni dei rispettivi ordinamenti", con il conseguente superamento del Regolamento del Garante n. 1/2013 concernente gli obblighi di pubblicità e trasparenza relativi all'organizzazione e all'attività dell'Autorità (delibera 1° agosto 2013, n. 380, doc. web n. 2573442) e della delibera 17 ottobre 2013, n. 455 (doc. web n. 2753146), recante la "Disciplina dei periodi di tempo di pubblicazione di dati, informazioni e documenti del Garante per la protezione dei dati personali".

Si è reso così necessario un aggiornamento dei contenuti della sezione "Autorità trasparente" del sito web del Garante ed è stato altresì predisposto l'aggiornamento del Programma triennale per la trasparenza e l'integrità rispetto al periodo 2014/2016.

24.3. *I prodotti informativi*

Sono stati diffusi 48 comunicati stampa e 15 *newsletter*. La *newsletter* del Garante è una pubblicazione periodica – giunta al suo XVI anno di diffusione (per un totale di 397 numeri e di 1.371 notizie) – che consente un approfondimento rispetto ai principali provvedimenti adottati dall'Autorità, alla sua attività in ambito europeo ed internazionale e alle molteplici iniziative legate alla diffusione della cultura della protezione dei dati personali. Tutte le notizie pubblicate vengono redatte a cura del Servizio relazioni con i mezzi di informazione, composte graficamente e completate con l'aggiunta di immagini per la versione web. La *newsletter* – che conta nella lista di distribuzione circa 6.500 destinatari – viene inviata via *e-mail* a redazioni, professionisti, operatori delle pp.aa., imprese e singoli cittadini che ne fanno richiesta (mediante l'opzione "Iscriviti alla *newsletter*" presente sul sito del Garante). È poi possibile consultare l'archivio tematico della *newsletter* che raccoglie i 16 anni di articoli prodotti, classificati per categorie.

24.4. *I prodotti editoriali e multimediali*

Tramite il Servizio relazioni con i mezzi di informazione l'Autorità svolge un'attività di promozione e divulgazione della conoscenza della disciplina sulla protezione dei dati personali utilizzando diverse forme di comunicazione. Negli anni ha ideato e realizzato numerosi prodotti (*vademecum*, opuscoli, piccole guide, schede informative, video, Dvd) su tematiche specifiche di largo interesse sociale, per informare il pubblico sui diritti riconosciuti dal Codice della *privacy* e svolgere un'azione di sensibilizzazione sul valore dei dati personali e sull'importanza della loro difesa.

Questa attività si è arricchita di nuovi prodotti. Per accrescere la consapevolezza degli utenti dei *social network* e offrire loro ulteriori elementi di riflessione e strumenti di tutela, è stato predisposto il *vademecum* "*Social privacy*. Come tutelarsi nell'era dei *social network*" (doc. web n. 3140082), un decalogo – inviato dal Garante a tutti i dirigenti scolastici – che aiuta ad utilizzare le opportunità offerte dal mondo digitale difendendosi dalle trappole della rete. Mantenendo la struttura agile del *vademecum* del 2009 ("*Social network*: attenzione agli effetti collaterali"), ad esso

sono stati aggiunti nuovi contenuti; particolare attenzione è stata rivolta a fenomeni, quali le false identità, il *sexting* e il cyberbullismo, che rischiano di creare pregiudizi, talora gravissimi, a tanti giovani. Il *vademecum* è stato distribuito in formato elettronico presso oltre 40.000 scuole statali e paritarie di 1° e 2° grado.

È stato poi realizzato il volume "Educare alla rete. L'alfabeto della nuova cittadinanza nella "società digitale" (doc. web n. 2893536) che raccoglie le principali campagne di comunicazione istituzionale realizzate dal Garante in questi anni, dirette alle famiglie, ai giovani, al mondo della scuola, alla sanità, alle amministrazioni pubbliche e alle imprese.

Traendo spunto dalle Linee guida in materia di pubblicità e trasparenza della p.a. è stato pubblicato l'opuscolo "La trasparenza sui siti web della PA" (doc. web n. 3134436).

Per quanto riguarda la produzione multimediale si è puntato ad innovare le strategie di comunicazione sperimentando nuovi canali, nuove tecniche e nuovi prodotti comunicativi pensati soprattutto per coinvolgere il pubblico più giovane. Con un investimento in dotazioni tecniche a bassissimo costo, il Garante ha prodotto (con riguardo a tutte le fasi di scrittura e adattamento dei testi, sceneggiatura, sviluppo dell'animazione e selezione/costruzione degli elementi visivi, scelta delle musiche e sincronizzazione, registrazione dei testi, adattamento audio, montaggio e postproduzione) contenuti audiovisivi di qualità, senza ricorrere a supporti esterni e utilizzando personale dell'Ufficio. Ai video *tutorial* e ai *vademecum* digitali già realizzati lo scorso anno, si è aggiunto il primo video prodotto *in house* dal Servizio relazioni con i mezzi di informazione, "*Cookie* e *privacy*: istruzioni per l'uso" (www.youtube.com/watch?v=Mut-YXSExnw), che ha riscosso un significativo successo da parte dell'utenza e ha permesso di definire le modalità operative per realizzare – in modo rapido, economico e qualitativamente adeguato – nuovi prodotti. Il coordinamento con l'Ufficio relazioni con il pubblico, inoltre, ha permesso di inserire il video nell'ambito di una campagna informativa ampia e articolata, che ha compreso una scheda di approfondimento (www.garanteprivacy.it/cookie) e FAQ tematiche su "Informativa e consenso sull'uso dei *cookie*" (provv. 8 maggio 2014, n. 229, doc. web n. 3585077). La campagna mira a sensibilizzare gli utenti di internet sull'invasività che i *cookie* – in particolare quelli di profilazione – possono avere nell'ambito della sfera privata nonché ad illustrare, in modo chiaro e sintetico, le misure di garanzia introdotte dall'Autorità con il provvedimento generale sull'uso dei *cookie* (doc. web n. 3118884). Nel video vengono, inoltre, indicate le accortezze che ogni utente può mettere in campo per limitare o bloccare del tutto la presenza di *cookie* durante la navigazione *online*. Il video è disponibile sia sul sito web dell'Autorità, sia sul canale You-tube aperto dal Garante (www.youtube.com/user/videogaranteprivacy), che già contiene altri filmati informativi su vari temi collegati alla tutela della *privacy online*.

Sono state predisposte e diffuse schede informative su varie tematiche: in occasione delle elezioni europee, la scheda "Elezioni europee. Le regole per il corretto uso dei dati" (doc. web n. 3126816), per ricordare a partiti politici e candidati le modalità per utilizzare correttamente i dati personali dei cittadini; quindi, sono stati formulati consigli per "navigare" sicuri durante le vacanze estive nella scheda "*Privacy* sotto l'ombrellone" (doc. web n. 3240343).

È stata progettata una nuova linea di strumenti informativi, denominata "Consigli flash", con contenuti caratterizzati da chiarezza e sinteticità espressiva, grafica innovativa e forte vocazione "*social*". I primi prodotti della nuova linea sono stati dedicati alla "*Privacy* su web e *social network*" e alle "Immagini *online*". Il progetto dei "Consigli flash" è stato accompagnato dall'ideazione di una strategia di

viralizzazione sui *social media* che appaiono particolarmente utili a supportare le necessità comunicative del Garante e le esigenze informative dell'utenza.

L'utilità e il gradimento di tutti i prodotti realizzati sono stati riscontrati dall'elevato numero di visualizzazioni sui *social network*, ma anche da vari articoli di apprezzamento apparsi sui giornali o su siti di esperti nel campo della comunicazione web.

Per la promozione dei video *tutorial* e per la valorizzazione di interviste e interventi audiovisivi dei membri del Collegio, come già detto, è attivo un canale Youtube del Garante. Nell'arco dell'anno i video sono stati visualizzati circa 29.000 volte. Sul *social network* LinkedIn sono state pubblicate circa 260 notizie relative all'attività del Garante e i *followers* hanno raggiunto la cifra di 2.100. La pagina LinkedIn è integrata con quella You-tube per una promozione incrociata e capillare dei contenuti e una moltiplicazione della visibilità comunicativa.

Del Dvd "Il Garante per la protezione dei dati personali" sono state pubblicate due nuove edizioni (la XXVI e la XXVII), rendendo disponibile un'ampia documentazione aggiornata sull'attività dell'Autorità, la legislazione nazionale ed internazionale, una sezione "temi" con schede informative multimediali su argomenti di particolare interesse. Utilizzando la tecnica del *cartoon* è stata realizzata ed inserita una nuova animazione multimediale sul tema della *privacy* nella vita condominiale. Come per le precedenti edizioni, nell'archivio sono disponibili tutte le pubblicazioni dell'Autorità, in forma integrale e nell'originaria veste editoriale. Le altre due aree tematiche "normativa" e "informazione", consentono di accedere ai testi normativi, ai comunicati stampa ed alla raccolta completa delle *newsletter*. In queste sezioni i documenti sono stati reimpaginati per la consultazione video.

24.5. *Gli incontri internazionali*

La consueta Conferenza internazionale delle Autorità per la protezione dei dati personali si è svolta a Balaclava (Mauritius) dal 23 al 24 ottobre 2014. L'Autorità è stata rappresentata dal segretario generale, Giuseppe Busia, che ha preso parte ad alcune sessioni: il seminario "*Digital Education*", incentrato sui criteri per garantire più efficaci politiche di sensibilizzazione sui temi della *privacy* da parte delle autorità per la protezione dei dati; il seminario sul "Progetto PHAEDRA", nel corso del quale sono stati illustrati i passi futuri per rafforzare la cooperazione internazionale nell'ambito della protezione dei dati. A conclusione dei lavori della 36ª Conferenza, le autorità partecipanti hanno adottato quattro risoluzioni su: internet *of things*, *big data*, *enforcement* e *privacy in digital age* (in merito v. *amplius* par. 23.2).

24.6. *Le manifestazioni e le conferenze*

L'attività dell'Autorità collegata a convegni, seminari ed altre iniziative di carattere divulgativo, ha suscitato rilevante interesse.

Giornata europea della protezione dei dati

Il 29 gennaio è stata celebrata l'annuale 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.

Nel 2014, il Garante ha voluto celebrare la Giornata europea organizzando un convegno dal titolo "Educare alla rete. L'alfabeto della nuova cittadinanza nella società digitale". Ai lavori, aperti dal presidente Soro, sono intervenuti Maria Chiara Carrozza, Ministro dell'istruzione, dell'università e della ricerca, Francesco Caio, Commissario di governo per l'attuazione dell'agenda digitale e Luigi Gubitosi, direttore generale Rai. "In una società che compra e vende informazioni e fa diventare merce la stessa persona la tutela della *privacy* diventa sempre più una questione di libertà. Si tratta di valori fondamentali che devono essere in primo luogo trasmessi ai giovani che più di altri possiedono le capacità per accedere e sfruttare in modo sempre più dinamico le opportunità offerte dalla società digitale, ma che spesso si muovono compulsivamente tra il modo digitale e quello reale senza rendersi pienamente conto del fatto che la vita vera è ovunque: in rete e fuori dalla rete". " La scuola – ha detto Soro nel suo intervento – potrebbe svolgere un ruolo di primo piano prevedendo, nell'ambito dei programmi scolastici, l'educazione digitale come materia di studio, a partire dalla scuola di base, con specifici progetti educativi che insegnino ai giovani il corretto modo di confrontarsi costruttivamente con le nuove tecnologie e le moderne forme espressive che le rete offre loro, al fine di promuovere una gestione consapevole di tutti gli aspetti della propria vita che vengono consegnati al mondo *online*". Secondo Soro, "il salto di qualità è capire che i dati personali contenuti nella rete sono la nostra vita e noi proteggiamo la nostra vita quando proteggiamo i nostri dati. Bisogna misurarsi con questa complessa fase di transizione e individuare e promuovere l'«educazione della persona digitale», una sorta di nuova educazione civica, rivolta a tutti i cittadini, agli operatori, agli utenti della rete senza distinzione di età o di ruoli".

Forum PA

Compatibilmente con tagli di spesa imposti dalla *spending review*, ma ritenendo importante un'azione di promozione dedicata espressamente agli operatori delle amministrazioni pubbliche, anche nel 2014 il Garante è stato presente all'appuntamento del *Forum* PA – il più grande incontro europeo dedicato all'innovazione e la modernizzazione del sistema pubblico italiano – svoltosi a Roma dal 27 al 29 maggio.

Nell'ambito del tema guida della XXV edizione, "Prendiamo impegni, troviamo soluzioni", l'Autorità ha toccato i temi della trasparenza *online* della p.a. oltre che la figura del *privacy officer*. In particolare, la vicepresidente, Augusta Iannini, ha partecipato al convegno "Trasparenza e *privacy*: due diritti dei cittadini" e, sullo stesso tema, ha tenuto il seminario "Ruoli e competenze delle istituzioni in materia di trasparenza della p.a." sottolineando l'importanza del diritto alla riservatezza, diritto fondamentale della persona riconosciuto dalla Carta europea dei diritti fondamentali come inviolabile; Licia Califano, componente dell'Autorità, ha illustrato le nuove "Linee guida del Garante *privacy* sulla trasparenza nella p.a." con le quali si è ricercato un corretto bilanciamento e un ragionevole equilibrio tra attuazione del principio di trasparenza e tutela della riservatezza; il segretario generale dell'Autorità, Giuseppe Busia, ha illustrato le principali novità contenute nella futura regolamentazione europea, con particolare riguardo al tema del *privacy officer*. Durante i tre giorni della manifestazione, presso lo *stand* del Garante il personale dell'Autorità ha risposto ai quesiti e distribuito le pubblicazioni curate dall'Ufficio; tra le novità, il test "Fatti *smart*" proposto ai visitatori per verificare la capacità di tutelare i propri dati personali nell'uso di *smartphone* e *tablet*.

Anci

Nell'ambito della XXXI Assemblea annuale Anci 2014 (tenutasi dal 6 all'8 novembre a Milano), il Garante ha organizzato la Tavola rotonda: "*Privacy* e trasparenza. Per una p.a. in rete attenta ai diritti" al fine di promuovere un dialogo tra le principali istituzioni coinvolte nell'attuazione del d.lgs. n. 33/2013 in materia di trasparenza amministrativa (Garante, Anac e Dipartimento della funzione pubblica, con

una attenzione per i Comuni, chiamati ad implementare gli obblighi di trasparenza), stimolando così un confronto produttivo in vista della delega correttiva e integrativa contenuta all'interno del disegno di legge del Governo in materia di riorganizzazione delle pp.aa. (AS 1577, art. 6). Ma pure si è inteso promuovere la diffusione e la conoscenza tra gli amministratori locali e il personale amministrativo degli enti locali delle Linee guida in materia di trasparenza adottate nel maggio 2014; i Comuni sono, infatti, in prima linea nell'applicazione degli obblighi di trasparenza e ad essi va dedicata una particolare attenzione, essendo tra i principali titolari del trattamento dei dati dei cittadini. Alla discussione hanno preso parte con un loro intervento: Licia Califano, componente del Garante; Carlo Colapietro, professore ordinario di Istituzioni di diritto pubblico all'Università Roma Tre; Marco Filippeschi, Sindaco di Pisa e rappresentante Anci per l'attuazione dell'Agenda digitale; Bernardo Giorgio Mattarella, Capo ufficio legislativo del Ministro per la semplificazione e la pubblica amministrazione; Ida Angela Nicotra, componente dell'Anac.

Altri convegni

Numerosi e interessanti i convegni e gli incontri ai quali ha partecipato il presidente Soro, molti dei quali legati alle tematiche legate alla sicurezza dei dati personali nello spazio digitale. Il 7 maggio, nella sala conferenze del Garante, si è svolto il convegno "*Cyber Security*: l'attuazione della strategia italiana". Il presidente Soro, con il suo intervento ha posto l'attenzione sulla necessità di mettere in sicurezza le banche dati strategiche e della p.a. e di puntare ad una raccolta dati che privilegi la qualità piuttosto che la quantità. "Non è vero – ha sostenuto Soro – che più dati si raccolgono e più si garantisce la sicurezza, né che la trasparenza è data da una raccolta massiva". "La protezione dei dati – ha continuato Soro – è uno straordinario fattore di competitività per il Paese; se è vero che senza sicurezza non c'è *privacy* (e nemmeno vera libertà), è anche vero il contrario: senza *privacy* non c'è sicurezza". Per queste ragioni "il Garante è da tempo impegnato nella promozione della sicurezza delle infrastrutture critiche nazionali e delle grandi banche dati, in particolare di quelle strategiche, la cui vulnerabilità metterebbe a rischio tanto l'interesse pubblico quanto i diritti fondamentali dei cittadini".

Il 16 giugno la Camera dei deputati ha organizzato una Conferenza dal titolo "Verso una Costituzione per internet" nel corso della quale autorevoli esperti hanno esaminato le evoluzioni della giurisprudenza e della normativa europea in materia di protezione dei dati. Ha aperto i lavori la presidente della Camera, Laura Boldrini. Nel suo intervento, il presidente Soro ha sollevato alcuni spunti di riflessione su temi cruciali: la caduta del confine tra virtuale e reale, le enormi concentrazioni di dati personali nelle mani di pochi monopolisti della rete, il ruolo dominante svolto dagli algoritmi che orientano le scelte e i comportamenti individuali in rete, la sorveglianza globale.

Il 18 novembre, presso la Sala del Cenacolo della Camera dei deputati, si è svolta la tavola rotonda "Trasparenza e *privacy*. Le questioni aperte e l'opportunità di un intervento normativo". All'incontro, organizzato dal presidente dell'Anac, Raffaele Cantone, e dal presidente dell'Autorità, Antonello Soro, ha partecipato la presidente della Commissione affari costituzionali del Senato, Anna Finocchiaro. "Il punto di partenza è che la trasparenza è il vero antidoto alla corruzione" ha spiegato Cantone. Ma "immettere *online*, sui siti istituzionali degli enti, troppi dati con un eccesso di trasparenza, rischia di determinare una «opacità per confusione», come l'ha definita Soro, che ha insistito invece sulla necessità di una "trasparenza democratica e non demagogica". Non è in discussione – ha aggiunto – la trasparenza come forma ineludibile dell'agire amministrativo ma, allo stesso tempo l'obbligo di trasparenza non sempre è garanzia di reale trasparenza". Dall'incontro è emersa l'esigenza di costituire un tavolo di lavoro congiunto, che ha preso l'avvio il 4 dicembre, tra l'Autorità (con

la partecipazione di Augusta Iannini e Licia Califano) e l'Anac (con la partecipazione di Angela Nicotra e Francesco Merloni) con lo scopo di addivenire ad un testo condiviso recante linee guida che possano chiarire l'estensione degli obblighi di trasparenza e pubblicazione dei dati bilanciandoli con le esigenze di riservatezza dei singoli.

Il 18 novembre "Etica e trasparenza nell'era dei *big data*" è stato il tema della tavola rotonda che si è tenuta a Roma in occasione della VI edizione del premio "Nostalgia del futuro", che vuole ricordare il presidente Fieg Giovanni Giovannini. Alla discussione ha preso parte il presidente Soro, il quale ha evidenziato come il crescente numero di dispositivi mobili utilizzati da ciascuno di noi, la diffusione dell'internet delle cose, l'interazione e lo scambio continuo di messaggi attraverso le reti sociali, abbiano rivoluzionato la possibilità di generare, condividere e trattare dati. Questa ingente quantità di informazioni, spesso carpite a inconsapevoli utenti, consente ai "giganti della rete" di effettuare valutazioni predittive sui comportamenti degli individui per condizionarne le scelte. Nuove forme di discriminazione possono derivare da profilazioni sempre più puntuali ed analitiche. Le sfide poste dai *big data* richiedono massima attenzione agli aspetti della sicurezza dei sistemi ma anche una riflessione sulla capacità effettiva delle norme giuridiche per la protezione della *privacy*.

A Perugia, dal 20 aprile al 4 maggio, al Festival internazionale di giornalismo si è parlato, tra l'altro, di "Odio in rete e cyberbullismo. Educazione digitale e libertà di parola". Il fenomeno del cyberbullismo è uno degli esiti più drammatici dell'uso della rete a scopi violenti o comunque offensivi, di cui sono vittime un numero sempre crescente di giovanissimi. Sul tema, caro al Garante, il presidente Soro ha osservato che "il problema della violenza in rete non si risolve unicamente con interventi normativi. Il cyberbullismo ha radici culturali e sociali non banali e non riconducibili ad una sola questione penale. È necessario anzitutto promuovere una reale educazione digitale che renda consapevoli, in modo particolare i ragazzi, delle opportunità ma anche dei rischi cui li espone la rete".

24.7. *Le relazioni con il pubblico*

Tramite l'Ufficio relazioni con il pubblico – al quale chiunque può rivolgersi di persona come pure per telefono, *e-mail* e posta – l'Autorità ha continuato a fornire informazioni e prestare attività di primo orientamento fornendo indicazioni sui profili connessi all'esercizio del diritto d'accesso e degli altri diritti riconosciuti alle persone fisiche dal Codice nonché, più in generale, chiarimenti sulle questioni attinenti alla tutela dei dati personali.

L'attività dell'Urp può essere ricondotta a tre principali macro-aree:

L'attività dell'Urp

- riscontro all'utenza: l'Ufficio esamina le istanze ricevute, valutando se al quesito può essere dato immediato riscontro, attraverso il rinvio a provvedimenti (generali o individuali) già adottati dal Garante, ed operando così come primo "filtro" rispetto alle istanze indirizzate all'Autorità;
- valutazione di novità ed "emergenze": in ragione dell'immediatezza del contatto con l'utenza, l'Urp costituisce un osservatorio privilegiato attraverso il quale, anche grazie ad apposita reportistica interna, l'Autorità può tempestivamente enucleare le tematiche, specie se emergenti, che più incidono sulla vita delle persone;
- informazione al cittadino: l'Urp, privilegiando la tempestività nei riscontri, rappresenta infine lo strumento di prima e diretta diffusione della conoscenza della normativa in materia di protezione dei dati personali e dei valori alla stessa sottesi ed in questa prospettiva, al fine di migliorare l'offerta infor-

mativa del Garante, ha curato la redazione di numerose FAQ (che si aggiungono alle modalità più tradizionali di informazione, quali guide, opuscoli, *vademecum*, pubblicazioni e altro materiale documentale). Pubblicate sul sito dell'Autorità, esse privilegiano le materie di più frequente segnalazione, quali il *marketing* telefonico (cfr. doc. web n. 3224019), le cd. telefonate mute (doc. web n. 3626528), l'esercizio dei diritti (doc. web n. 3497679) e l'uso dei *cookie* (doc. web n. 3585077). A quest'ultimo proposito, con una tecnica di comunicazione diretta e inusuale per l'Autorità, è stato realizzato anche un video *tutorial*, veicolato anche attraverso il canale ufficiale del Garante sulla piattaforma di You-tube.

Indicatori numerici

I dati statistici riguardanti l'attività dell'Urp (compiutamente indicati nella sez. IV, tab. 20) confermano la persistente attenzione rispetto al tema della tutela dei dati personali. Nell'ambito dell'attività di *front office*, infatti, i contatti registrati nel periodo di riferimento sono complessivamente pari a 33.191, per lo più per via telefonica o per posta elettronica (18.717 *e-mail*). Gli affari definiti sono stati 586, mentre i visitatori ricevuti presso la sede dell'Ufficio sono stati 363.

Tematiche d'interesse

Tra i temi portati all'attenzione dell'Autorità tramite l'Urp si evidenzia, anche per il 2014 (cfr. sez. IV, tab. 21), quello del *marketing* (38% delle *e-mail* pervenute). Il settore delle segnalazioni più numerose (e non di rado risentite), nonostante l'istituzione, da oltre quattro anni, del Registro pubblico delle opposizioni, è quello del *telemarketing* (27% circa), che suscita, per la frequenza delle chiamate promozionali indesiderate (a qualunque ora del giorno) e delle modalità di contatto (spesso aggressive), uno stato di generalizzata insofferenza nell'utenza.

Frequentemente segnalate sono state anche l'attività di *marketing* svolta attraverso strumenti informatici (sms e *e-mail*), la ricezione di fax promozionali non richiesti nonché la ricezione delle cd. telefonate mute (cfr. par. 12.1); con particolare riferimento a queste ultime, è stato ripetutamente lamentato il mancato rispetto da parte degli operatori delle prescrizioni impartite dal Garante nel provvedimento del 20 febbraio 2014, n. 83 (doc. web n. 3017499), senza considerare però che il termine concesso per la loro attuazione sarebbe scaduto soltanto ad ottobre.

Nell'ambito delle richieste di intervento all'Autorità relative all'attività svolta dai gestori telefonici e telematici, una questione particolarmente sentita riguarda l'attivazione di servizi a pagamento non richiesti sulle utenze di telefonia mobile. Al riguardo, gli utenti lamentano come anche il solo "sfiorare" certi *link* presenti nelle pagine web visitate con lo *smartphone* porti all'attivazione di servizi a pagamento (con conseguenti addebiti e difficoltà nella disattivazione). Sul tema, da tempo all'attenzione del Garante, sono in corso accertamenti, resi complessi anche dalla molteplicità e varietà dei soggetti a vario titolo coinvolti.

Permane inalterata l'attenzione sulla videosorveglianza (in particolare nel contesto lavorativo, condominiale o in relazione alle *dashcam*), sul trattamento dei dati personali nella gestione del rapporto di lavoro e su quello connesso allo svolgimento dell'attività giornalistica.

Le richieste in materia di videosorveglianza (962 *e-mail*) hanno avuto ad oggetto essenzialmente gli adempimenti previsti dal provvedimento generale dell'8 aprile 2010 (doc. web n. 1712680), con particolare riferimento ai casi in cui è necessario richiedere una verifica preliminare all'Autorità (art. 17 del Codice).

Significativo permane il numero delle segnalazioni e dei quesiti relativi ai trattamenti di dati personali nell'ambito dei rapporti di lavoro pubblico e privato (668 *e-mail*). Le tematiche di maggiore interesse continuano ad essere quelle relative all'utilizzo di internet e posta elettronica sul posto di lavoro, al trattamento di dati sensibili correlato al riconoscimento di permessi o benefici, al controllo a distanza dei lavo-

ratori, con particolare riguardo al tema della geolocalizzazione effettuata mediante l'utilizzo dei nuovi strumenti di lavoro (quali, ad es., *tablet* e *smartphone*), al rilevamento delle presenze dei lavoratori mediante sistemi tecnologicamente avanzati.

Con specifico riferimento ai trattamenti di dati biometrici, anche in ambito lavorativo, ampia eco ha avuto il provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014, n. 513 (doc. web n. 3556992).

Tematica che riscuote crescente interesse è quella relativa al trattamento dei dati nell'ambito dei *social network*. La diffusione di queste nuove forme di comunicazione e condivisione delle informazioni determina la disponibilità *online* di (più o meno ampi) "vissuti" personali di individui (in larga misura minori) che, più o meno consapevolmente, rinunciano al riserbo sulla propria sfera personale, spesso disvelando informazioni intime e perfino di natura sensibile. Forti criticità si incontrano nel fornire tutela in tali contesti, poiché l'applicabilità della normativa italiana rispetto ai trattamenti di dati coinvolti trova un limite nel fatto che essi spesso vengono effettuati da titolari stabiliti all'estero (e sovente in Paesi terzi).

Si evidenzia inoltre un interesse sempre maggiore per le tematiche relative al trattamento dei dati personali nell'ambito del web in generale (1.192 *e-mail*), anche in relazione alle novità introdotte dalla nota sentenza nel caso *Google Spain* che ha dischiuso scenari nuovi in termini di tutela dei dati personali in rete e ha determinato un aumento degli utenti che si sono rivolti all'Autorità (in merito v. *amplius* par. 10.4 e 23).

Resta immutato l'interesse per il tema relativo a protezione dei dati e giornalismo, con riferimento alla corretta gestione dei cd. archivi storici *online* dei quotidiani, anche alla luce delle indicazioni fornite dalla Cassazione (Cass. civ., Sez. III, 5 aprile 2012, n. 5525).

Altrettanto significative, soprattutto per la particolare delicatezza dei temi trattati, sono state le richieste relative al rapporto tra la tutela dei dati personali e l'esercizio della libertà di manifestazione del pensiero, nonché al tema della divulgazione di immagini fotografiche, spesso riguardanti minori, sul web.

Gli utenti inoltre hanno dimostrato grande attenzione anche nei confronti del provvedimento dell'8 maggio 2014, n. 229 in materia di *cookie* (doc. web n. 3118884), con il quale il Garante ha individuato le modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso di tali strumenti. La maggior parte delle richieste relative a questo argomento ha riguardato: l'obbligo di realizzare il *banner* previsto dal provvedimento per informare gli utenti; il rapporto tra il gestore del sito e le cd. terze parti; la gestione dei *cookie analytics*, ossia dei *cookie* utilizzati per effettuare analisi statistiche sull'uso dei siti.

Altro settore su cui si è fortemente focalizzata l'attenzione degli utenti è quello della trasparenza nella pubblica amministrazione. Gli obblighi derivati dall'adozione del cd. decreto trasparenza (d.lgs. n. 33/2013) hanno infatti evidenziato numerose problematiche interpretative strettamente connesse alla tutela della riservatezza sia delle cariche elettive, sia di quanti, a vario titolo e con riguardo a predefiniti *set* di informazioni, vedono i dati personali a sé riferiti oggetto di pubblicazione in internet. Gli aspetti problematici più ricorrenti hanno riguardato: l'obbligo di pubblicazione dei redditi e dei dati patrimoniali di sindaci, consiglieri e assessori comunali, provinciali e regionali; le modalità di pubblicazione degli elenchi di soggetti beneficiari di sovvenzioni o contributi; la pubblicazione nell'albo pretorio di determine indicizzate in rete.

Su questi temi le indicazioni contenute nelle "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri

enti obbligati" del 15 maggio 2014, n. 243 (doc. web n. 3134436) hanno consentito in molti casi di rendere risposta ai quesiti formulati, pur residuando aspetti che ancora richiedono approfondimenti.

Va ricordato inoltre un costante interesse per le questioni attinenti alla materia dell'accesso, da parte sia dei cittadini sia dei consiglieri comunali, ai documenti amministrativi e agli atti degli enti locali, per i quali però, come noto, l'Autorità non ha competenza ad esprimersi in ordine al rilascio o meno degli atti richiesti.

Numerose sono state le richieste provenienti dai gestori di pubblici esercizi, relative alla liberalizzazione dell'accesso alla rete *WiFi* operata lo scorso anno dal d.l. n. 69/2013, convertito, con modificazioni, dalla l. n. 98/2013. In alcuni casi, si sono riscontrate preoccupazioni con particolare riferimento all'eventuale necessità di identificare gli utilizzatori della rete nei casi di reati commessi tramite la connessione in oggetto.

Un costante interesse si è potuto registrare nelle richieste di informazioni degli utenti relative agli strumenti di tutela approntati dal Codice (1.358 *e-mail*). Il pubblico chiede di conoscere innanzitutto le sostanziali differenze tra i vari strumenti che il Codice mette a disposizione (segnalazioni, reclami e ricorsi) e ha mostrato un elevato gradimento nell'invio di note di chiarimento circa le corrette modalità per esercitare strumenti di tutela per i quali la legge richiede alcune formalità, come nel caso dello strumento del ricorso, ora chiarite mediante FAQ (doc. web n. 3497679).

Grande interesse continuano a suscitare le problematiche connesse ai sistemi di informazioni creditizie e le questioni attinenti alla possibilità di accedere ai dati bancari invocando la normativa in materia di protezione dati, in contrapposizione al diritto di ottenere copia della documentazione bancaria sulla base dell'art. 119, d.lgs. n. 385/1993 (Testo unico delle leggi in materia bancaria e creditizia). In considerazione dell'ampio interesse sul punto, sono state predisposte delle FAQ (doc. web n. 3557649) che chiariscono la sostanziale differenza tra i due strumenti. Altri temi d'interesse riguardano la pertinenza e non eccedenza delle informazioni richieste dalle banche circa l'applicazione della normativa in materia di antiriciclaggio (d.lgs. n. 231/2007) e le comunicazioni a terzi di informazioni bancarie.

In relazione all'attività di recupero del credito, si confermano le medesime criticità, già emerse lo scorso anno, relative alle modalità utilizzate per contattare i debitori e sollecitare i pagamenti. Sempre molto frequente è, infatti, il ricorso a modalità non corrette e comunque non corrispondenti a quelle indicate da tempo dall'Autorità, quali visite al domicilio o sul luogo di lavoro del debitore, sollecitazioni telefoniche non solo presso i suoi recapiti, ma anche presso familiari, vicini di casa, datori di lavoro.

Si registra, infine, un notevole incremento dei quesiti in materia di trasferimento all'estero di dati personali, con particolare riferimento al ruolo e alle effettive responsabilità della figura del rappresentante nel territorio dello Stato.

24.8. *Il Servizio studi e documentazione*

Il Servizio studi ha coordinato la predisposizione del testo della Relazione annuale 2013: essa, oltre a costituire un importante adempimento (previsto dall'art. 154, comma 1, lett. *m*), del Codice), in ragione della completezza nella rappresentazione dell'attività (provvedimentale e non) dell'Autorità nell'anno solare di riferimento, costituisce un effettivo esercizio di trasparenza in relazione all'attività svolta, rendendone pienamente edotti non solo i suoi destinatari naturali, Parlamento e Governo, ma pure la collettività. Inoltre, grazie ai puntuali riferimenti contenuti nel

testo, la relazione rappresenta uno strumento conoscitivo prezioso per gli interlocutori istituzionali dell'Autorità (titolari del trattamento, operatori giuridici, ricercatori, etc.), che trovano concentrata in un'unica sede (immediatamente accessibile) la memoria storica di quanto fatto. Arricchendo le informazioni di natura statistica e rendendo immediatamente percepibile e (per quanto possibile) "quantificabile" in schede di sintesi la multiforme attività svolta, si è altresì mirato a realizzare una comunicazione più immediata, dal punto di vista del lettore (oltre che a beneficio degli infomediari), dell'operato dell'Autorità, in particolare, dell'attività provvedimentale, sanzionatoria e comunicativa nonché degli impegni assolti nel contesto europeo ed internazionale.

Il Servizio ha altresì svolto sistematicamente attività di documentazione interna (in relazione a novità normative, giurisprudenziali e dottrinali incidenti nel settore della protezione dei dati personali) ed effettuato studi ed approfondimenti sulle materie all'attenzione dell'Autorità (spesso funzionali all'istruttoria di provvedimenti di carattere generale) o su questioni comunque di interesse mediante note di approfondimento e *dossier* (assicurandone il costante aggiornamento).

Ha inoltre fornito, a mezzo di atti interni, elementi di valutazione ai fini della formulazione dei pareri richiesti dalla Presidenza del Consiglio dei ministri e dal Dipartimento per i rapporti con il Parlamento per l'eventuale impugnazione davanti alla Corte costituzionale delle leggi regionali ritenute di dubbia conformità limitatamente alla materia della protezione dei dati personali (cfr. par. 3.5) e delle risposte agli atti di sindacato ispettivo (cfr. par. 3.3).

Nell'ambito delle risorse disponibili presso l'Autorità, il Servizio ha infine curato la formazione esterna in materia di protezione dei dati personali: ciò è avvenuto sia attraverso l'organizzazione e la partecipazione a due seminari presso la sede del Garante in materia di trasparenza amministrativa (7 luglio e 15 ottobre), cui hanno assistito complessivamente 238 partecipanti, sia svolgendo attività formative fuori sede (con la cooperazione di altro personale dell'Autorità) nell'ambito del protocollo stipulato con la Scuola superiore del Ministero dell'economia e delle finanze "E. Vanoni" (con la partecipazione complessiva di circa 175 persone).

24.9. *La Biblioteca*

La Biblioteca nasce nel 2001 e rappresenta un'articolazione della Segreteria generale. Il suo compito istituzionale consiste nel raccogliere, organizzare, classificare con criteri bibliografici, conservare, gestire e valorizzare le pubblicazioni italiane e straniere attinenti alla disciplina della protezione dei dati nonché alle tematiche dei diritti e delle libertà fondamentali, della dignità, della riservatezza e della identità personale.

Il patrimonio della Biblioteca, costituito da ca. 24.000 titoli (con 15.000 volumi, 7.500 dei quali in lingua straniera), è arricchito da un Fondo speciale, donato dal prof. Rodotà e incrementato nel corso del tempo, che raccoglie ca. 2.000 documenti di particolare pregio da un punto di vista storico e retrospettivo sui temi del diritto alla riservatezza in Italia e sul *right to privacy* nella tradizione giuridica anglo-americana; un altro Fondo di ca. 400 titoli è stato donato dal cons. Buttarelli. Presso la Biblioteca esiste inoltre un deposito di ca. 200 tesi italiane di laurea e di dottorato in materia di protezione dei dati. Dal 2004 sul sito web della Biblioteca in intranet è consultabile il catalogo OPAC che contiene 5.393 monografie e 90 periodici. Le acquisizioni successive al 2004 vengono pubblicate in formato elettronico con bollettini quadrimestrali.

La Biblioteca – ulteriormente valorizzata dal completamento della catalogazione in OPAC e la sua immissione in internet – è nata per supportare le attività di informazione, di ricerca e di studio dell'Autorità; i servizi all'utenza esterna sono pertanto complementari (anche in ragione delle risorse disponibili) rispetto a questo fine istituzionale.

Nel contesto generale di razionalizzazione della spesa (cfr. par. 25.2), l'Ufficio ha dovuto attivare un'opzione di recesso della sala conferenze che ha interessato anche i locali della Biblioteca. Il successivo spostamento di quest'ultima in altri spazi dell'Autorità ha ridotto ad un'unica sala di consultazione le tre sale originarie, con il trasferimento nei magazzini di ca. il 75% delle collezioni possedute (attualmente il patrimonio a vista risulta collocato su ca. 107 metri lineari rispetto ai ca. 225 metri lineari antecedenti, mentre le collocazioni nei magazzini occupano ca. 375 metri lineari).

La Biblioteca rappresenta una singolarità a livello italiano ed europeo sotto numerose angolazioni. Il Garante italiano risulta difatti unico nella UE ad avere istituito una biblioteca specialistica di grandi dimensioni sui temi della *privacy* e della protezione dei dati. La stessa politica delle acquisizioni, rivolta anche all'incremento del patrimonio sul piano storico e retrospettivo, tramite interventi sul mercato librario internazionale dell'usato, assume un particolare rilievo nel panorama delle istituzioni bibliotecarie.

In termini di comparazione e per l'utilità dei riscontri statistici (aggiornati al 31 marzo 2015), il sistema SBN cataloga 1053 monografie (622 in italiano) con il vocabolo "*privacy*" nel titolo; 149 monografie con la stringa di "protezione dei dati"; 163 monografie con l'espressione di "*data protection*"; 339 monografie (265 in italiano) sotto il soggetto di "Diritto alla riservatezza". Il Polo Bibliotecario Parlamentare cataloga sotto il soggetto "riservatezza (diritto)" 930 *record* (462 in italiano): 574 *record* (222 in italiano) la Biblioteca della Camera dei deputati e 356 *record* (240 in italiano) la Biblioteca del Senato. I *record* aventi il vocabolo "*privacy*" nel titolo sono 200 (111 alla Camera e 89 al Senato). In Germania, la *Deutsche Nationalbibliothek* conta 1699 *record* (783 volumi) con ricerca sul vocabolo "*privacy*" e 4.619 *record* (2.914 volumi) con ricerca sul vocabolo "*Datenschutz*". Negli Stati Uniti, la principale biblioteca giuridica mondiale, la *Harvard Law School Library*, cataloga sotto il soggetto "*privacy*" 8.498 monografie (7570 volumi), con 1.517 monografie (e 946 volumi) pubblicate nel biennio 2013-2014. Le monografie in italiano sono 86. Sotto il soggetto "*Privacy, Right of*" risultano 4.599 monografie (4.309 volumi); sotto il soggetto "*Privacy, Right of – Italy*" 61 monografie; sotto il soggetto "*Data protection*" 3.473 monografie; sotto il soggetto "*Freedom of Information*" 2.979 monografie. La *Yale Law School* cataloga sotto il soggetto "*Privacy, Right of*" 1.890 *record*; sotto "*Privacy, Right of – Italy*" 46 *record*; "sotto "*Data protection*" 661 *record*; sotto "*Freedom of Information*" 920 *record*. Infine, la *Library of Congress* cataloga sotto il soggetto "*Privacy, Right of*" 3.798 *record*; sotto "*Privacy, Right of – Italy*" 92 *record*; "sotto "*Data protection*" 2.761 *record*; sotto "*Freedom of Information*" 2.562 *record*.

Nel 2014 i servizi all'utenza interna ed esterna sono stati dapprima ridotti e poi temporaneamente sospesi a causa degli impegni di organizzazione del trasloco. Questi i dati annuali relativi agli utenti interni: 1.207 i documenti richiesti in lettura; 278 i prestiti; 980 le richieste di fotoriproduzioni; 77 i casi di assistenza bibliografica (22 *online*); 48 le riproduzioni di documenti con inoltro in formato elettronico (*Document Delivery*). Questi i dati sul pubblico esterno: 22 le autorizzazioni alla frequentazione; 278 i titoli consegnati in lettura; 220 le richieste di fotoriproduzioni; 74 i casi di assistenza bibliografica *online*; 102 gli invii di *Document Delivery*.

La consultazione del catalogo OPAC sulla Intranet ha registrato una leggera variazione rispetto al 2012 (5.904 contatti contro 6014). Per quanto riguarda i *database* giuridici gestiti sulla Intranet attraverso il sito web della Biblioteca, i dati di consultazione da parte dei dipendenti dell'Autorità rivestono speciale importanza come indicatori dell'elaborazione che precede la messa a punto dei "prodotti" dell'Ufficio. Gli elaborati statistici indicano che il numero totale dei documenti consultati nel 2014 si avvicina al traguardo simbolico di ca. 100.000. Il *database* con il più elevato conteggio ha registrato 6.814 sessioni di lavoro (6.529 nel 2013, 5.828 nel 2012, 4.889 nel 2011 e 4.052 nel 2010) e 83.831 documenti consultati (75.525 nel 2013, 60.419 nel 2012, 60.141 nel 2011 e 48.112 nel 2010), per una media giornaliera lavorativa di ca. 30 connessioni e 364 documenti (28 connessioni e 337 documenti nel 2013).

III - L'Ufficio del Garante

25 La gestione amministrativa dell'Ufficio

25.1. *Il bilancio e la gestione finanziaria*

La gestione del bilancio ha generato un avanzo di circa 1,8 milioni di euro il cui dato, tuttavia, fa registrare una contrazione di oltre il 50% rispetto al risultato conseguito nel precedente esercizio. Dal raffronto delle due annualità emerge che il risultato finanziario della gestione 2014 è più contenuto rispetto a quello conseguito nel 2013 per ragioni ascrivibili prevalentemente alla riduzione delle entrate e ad una tendenziale contrazione delle spese di funzionamento.

Le somme acquisite al bilancio del Garante sono state destinate in via prioritaria e in misura pressoché prevalente al sostenimento degli oneri obbligatori, funzionali allo svolgimento dei compiti istituzionali, oltre che 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.

Anche per il 2014 la parte prevalente delle fonti di finanziamento dell'Autorità è costituita da trasferimenti, di cui la misura più significativa, prevista sul piano legislativo in 12 milioni di euro, è posta a carico di sei autorità indipendenti. Tale modalità di finanziamento, operante dall'anno 2011 e prevista fino al 2016, è stata dettata dalla necessità di fare fronte alla sostanziale impossibilità per l'Autorità di rivolgersi ad uno specifico "mercato di riferimento" da cui attingere le risorse finanziarie in misura sufficiente a sostenere le proprie esigenze di spesa. Peraltro, è doveroso precisare che il legislatore, oltre a individuare tale fonte di finanziamento, ha anche disposto, nel corso degli anni, la progressiva riduzione del trasferimento a carico dei fondi erariali che sarebbero stati comunque dovuti a copertura delle spese di funzionamento dell'Autorità, in attuazione dell'art. 156, comma 10, del Codice.

In aggiunta alle difficoltà amministrative verificatesi più volte nel corso di questi anni, dovute a ritardi nel trasferimento delle somme da parte di alcuni soggetti debitori, l'andamento dell'anno 2014 ha fatto registrare per la prima volta una riduzione del finanziamento di 2 milioni di euro rispetto alle risorse complessivamente previste dal legislatore. Infatti, la specifica disposizione legislativa che ne dispone l'erogazione è stata disapplicata dall'Autorità per le garanzie nelle comunicazioni, all'esito di controversie promosse dagli operatori appartenenti al proprio settore di regolazione, tenuto conto di alcune decisioni assunte dal giudice amministrativo. Ciò richiede l'adozione di idonee misure legislative affinché il Garante possa avvalersi di ordinarie forme di finanziamento, analogamente a quanto previsto per le principali autorità indipendenti, valorizzandone l'autonomia gestionale ed assicurando la disponibilità delle risorse con procedure che ne assicurino la stabilità finanziaria, anche al fine di pianificare la propria attività istituzionale in base a principi ispirati alla corretta programmazione gestionale.

Quanto ai fondi gravanti sulle risorse erariali a titolo di contributo statale ordinario di funzionamento, si evidenza che gli stessi – proprio in ragione della modifica della struttura del finanziamento innanzi illustrata – rappresentano una misura più contenuta del totale delle entrate, pari al 36,5%, e la loro entità acquisita nell'anno, corrispondente a 7,6 milioni di euro, risulta ridotta di 0,8 milioni di euro (-9,05%) rispetto alle analoghe somme trasferite dal bilancio erariale nel precedente esercizio, a conferma di una costante riduzione delle risorse erariali destinate al funzionamento dell'Autorità che si registra ormai da alcuni anni.

Da ultimo, misure meno rilevanti di entrata sono costituite da diritti di segreteria e da proventi per sanzioni amministrative irrogate nell'ambito delle attività di accertamento e di controllo demandate dalla legge all'Autorità.

Le entrate totali di cui il Garante ha acquisito il diritto alla riscossione nel 2014 sono state pari complessivamente a 21 milioni di euro, il cui importo fa registrare una flessione rispetto al precedente esercizio pari a 2 milioni di euro. La parte preponderante degli importi per i quali è maturato nell'anno il diritto alla loro acquisizione è stata riscossa nell'esercizio di competenza mentre per una minima parte, a causa della normale dinamica gestionale, l'incasso è stato rinviato all'esercizio successivo.

Sotto il versante della spesa, gli oneri complessivamente impegnati ammontano a 19 milioni di euro. Dal raffronto con i dati consuntivi dell'esercizio precedente emerge una riduzione delle spese di funzionamento, la cui variazione è stata influenzata anche dalle misure di contenimento della spesa pubblica adottate sul piano legislativo nel 2014.

Si tratta, in primo luogo, degli interventi contenuti nel d.l. n. 66/2014 con cui, tra l'altro, è stata ampliata, dal 10 al 15%, la misura della riduzione della spesa per consumi intermedi, cui il Garante ha dato applicazione nei termini prescritti.

Ulteriori norme di contenimento della spesa, parimenti applicabili alle autorità indipendenti, hanno determinato una revisione delle politiche gestionali e di bilancio. In particolare, l'art. 22, d.l. n. 90/2014 ha inciso, a vario titolo, in tema di riduzione della spesa. Va precisato, tuttavia, che non tutte le norme ivi contenute hanno spiegato effetti direttamente a carico dell'esercizio in questione, posto che per una parte di esse il risultato è atteso a partire dal bilancio 2015.

Unitamente alla puntuale applicazione delle disposizioni legislative in argomento, il Garante ha continuato a tenere conto dei precedenti provvedimenti che comunque hanno comportato una gestione attenta delle risorse finanziarie, in linea con le esigenze di un generale contenimento della spesa.

Dal raffronto dei dati dell'esercizio 2014 con quelli dell'annualità precedente emerge che, a fronte di una riduzione delle spese di funzionamento, si è reso necessario incrementare alcune spese in conto capitale, non più rinviabili, per 0,3 milioni di euro per esigenze ascrivibili, in larga parte, alla necessità di acquisizione di licenze nel campo informatico e sono state impegnate risorse per 0,4 milioni di euro per dare corso ad un trasferimento straordinario in relazione alla definizione di una transazione con il Dipartimento della protezione civile.

Con riferimento alla spesa complessiva, rispetto alle stime iniziali assunte in sede di previsione annuale, gli oneri effettivamente impegnati hanno fatto registrare una riduzione di oltre 3,7 milioni di euro, alla cui economia ha concorso principalmente la realizzazione di minori spese correnti, prioritariamente quelle per il personale, essendo stato scelto di posticipare agli anni successivi il completamento della pianta organica.

L'Ufficio ha proseguito nel solco di una gestione virtuosa, ad esempio, mantenendo l'azzeramento delle auto di servizio (v. par. 25.3) e continuando a non fare alcun ricorso a consulenze nel corso dell'esercizio.

Per quanto attiene agli emolumenti corrisposti al personale, in attuazione di puntuali disposizioni legislative e nel rispetto dell'autonomia che la legge riserva all'Autorità, si è registrata una diminuzione della spesa, ascrivibile al contenimento della componente accessoria della retribuzione ed alla sostanziale invarianza di quella fissa.

Tali interventi non hanno comunque consentito di far registrare, in termini complessivi, economie di spesa maggiormente tangibili a vantaggio del bilancio, atteso che la spesa prevalente riguarda oneri, in massima parte aventi carattere fisso e continuativo, non comprimibili oltre determinati margini su iniziativa dell'amministrazione. 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.

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 (cfr. sez. IV, tab. 24) riassume sinteticamente la gestione dell'Autorità nel 2014, ponendo a raffronto i valori finanziari di competenza con quelli corrispondenti dell'esercizio precedente. Essa espone, in particolare, le fonti di finanziamento complessive dell'anno, con evidenziazione degli importi, a carico del bilancio dello Stato, ascrivibili a mero trasferimento per il funzionamento dell'Ufficio. Per quanto riguarda la spesa, l'onere complessivo sostenuto 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, da quella per investimento, nonché per restituzioni in favore dell'erario. 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.

25.2. *L'attività contrattuale e la gestione economale*

Anche l'attività contrattuale dell'Autorità si è svolta in attuazione degli obiettivi generali fissati dal Garante continuando a perseguire le finalità di miglioramento in termini di efficienza e risparmio. Tale attività è stata profondamente influenzata dalle riforme normative intervenute nel corso dell'anno, relativamente agli aspetti contrattuali e, in termini più ampi, all'assetto generale delle autorità amministrative indipendenti.

Tra tali innovazioni vanno ricordate, in particolare, quelle introdotte dal d.l. n. 90/2014, poi convertito in legge, con modificazioni, dall'art. 1, comma 1, l. 11 agosto 2014, n. 114, che hanno stabilito, fra l'altro, che le autorità indipendenti gestiscano "i servizi strumentali in modo unitario, mediante la stipula di convenzioni o la costituzione di uffici comuni ad almeno due organismi" (art. 22, comma 7); in particolare, entro il 31 dicembre 2014, le predette autorità avrebbero dovuto organizzare in tal modo almeno tre dei seguenti servizi: affari generali, servizi finanziari e contabili, acquisti e appalti, amministrazione del personale, gestione del patrimonio, servizi tecnici e logistici, sistemi informativi ed informatici. Dall'applicazione di tale disposizione dovrebbero derivare, entro l'anno 2015, risparmi complessivi pari ad almeno il 10% della spesa complessiva sostenuta dagli stessi organismi per i medesimi servizi nell'anno 2013.

Al fine di dare applicazione a tale previsione normativa si sono tenuti incontri con altre autorità potenzialmente interessate ad avviare una gestione in comune di tali servizi, che hanno condotto alla stipula, in data 17 dicembre 2014, di una convenzione fra Autorità per le garanzie nelle comunicazioni, Autorità per l'energia elet-

trica il gas e il sistema idrico e il Garante, grazie alla quale, con l'obiettivo di perseguire i richiesti risparmi, si è deciso di avviare la prevista collaborazione nella gestione dei servizi relativi ad "affari generali"; "acquisti e appalti" e "amministrazione del personale".

Fra le ulteriori novità normative aventi effetto sul settore considerato, vanno richiamati l'art. 1, comma 450, l. 27 dicembre 2006, n. 296, così come integrato dall'art. 22, comma 8, lett. *b*), d.l. 24 giugno 2014, n. 90, che ha esteso anche alle autorità indipendenti alcuni obblighi relativi all'utilizzazione della piattaforma di Consip s.p.a. (in particolare, rendendo obbligatorio il ricorso al Mercato elettronico della pubblica amministrazione-Mepa, fermi restando gli ulteriori, previgenti obblighi); nonché, sotto altro profilo, l'art. 24-*bis*, d.l. n. 90/2014 che ha esteso alle autorità indipendenti gli obblighi di trasparenza previsti dal d.lgs. n. 33/2013. Ciò ha determinato il superamento del previgente Regolamento interno del Garante n. 1/2013, inducendo l'Ufficio ad una generale revisione delle attività finalizzate alla corretta attuazione delle nuove disposizioni, effettuata di concerto con gli uffici interessati.

Per quanto specificamente attiene all'attività contrattuale, nel periodo in questione, si è registrata una diminuzione del numero di contratti stipulati rispetto all'anno precedente, beneficiando degli esiti delle procedure selettive esperite in precedenza, bandite generalmente per un periodo più ampio rispetto al passato.

Fra i dati più significativi, meritano di essere menzionate l'adesione a due Convenzioni Consip ("Licenze Microsoft GOL" e fornitura di energia elettrica) e la proroga della Convenzione "Telefonia mobile 5" effettuata nelle more dell'attivazione della nuova Convenzione da parte della medesima Centrale di committenza.

Per quanto riguarda l'utilizzazione del Mepa, sono state esperite alcune procedure selettive mediante richiesta di offerta (RdO), volte principalmente all'acquisto di prodotti o servizi tecnologici, che sono state concluse con sensibili ribassi rispetto alla base d'asta (fino al 27%). Lo strumento comparativo della RdO è stato utilizzato, come in passato, anche per importi sensibilmente inferiori a quelli previsti obbligatoriamente dalla legge (40.000 euro) al fine di garantire la massima concorrenza, la trasparenza e l'economicità degli acquisti.

Sono stati inoltre effettuati circa trenta affidamenti diretti, per importi ed acquisti di portata minore (atti di cd. micro-contrattualistica), con una spesa complessiva annua pari a circa 70.000 euro ed una media di circa 2.400 euro per singolo contratto. Tali affidamenti sono stati effettuati principalmente in relazione ad esigenze di importi esigui, in ragione della maggiore economicità della procedura ed in relazione al bene/servizio richiesto individuando, laddove possibile, il miglior offerente sul Mepa.

A seguito di una procedura selettiva andata deserta è stata poi affidata, previa ulteriore ricerca di mercato, la fornitura dei giornali per l'Autorità.

Alcuni contratti in essere sono stati prorogati, nei termini previsti dagli originari atti di gara (ad es. servizio di vigilanza), tenendo anche conto dell'istruttoria in corso relativa alla sede dell'Autorità.

Fermo quanto sopra riguardo alle RdO Mepa, è stata altresì effettuata una procedura di cottimo fiduciario per la fornitura di banche dati giuridiche, all'esito di un'attenta disamina finalizzata a sistematizzare tali acquisti, effettuata in collaborazione con gli uffici interessati; la procedura è stata aggiudicata con la realizzazione di un significativo ribasso, pari a circa il 34% rispetto alla base d'asta.

Inoltre, nel corso dell'anno sono stati eseguiti affidamenti diretti ai sensi dell'art. 57, comma 2, lett. *b*), del Codice dei contratti pubblici (cd. fornitore unico) riguardanti principalmente la partecipazione dell'Autorità ad eventi di settore e prodotti o servizi informatici necessari alla regolare prosecuzione delle attività dell'Ufficio

(ad es.: partecipazione all'Assemblea nazionale Anci 2014 e al Forum P.A. 2014, rinnovo del servizio di accesso alle banche dati del sistema camerale e manutenzione relativa al sistema di "protocollo informatico e gestione documentale *folium*" ed attività sistemistiche).

Si segnala, in particolare, l'affidamento al consorzio Cineca – interamente partecipato da soggetti pubblici e privo di finalità lucrative – di un contratto relativo a servizi di sviluppo *software* per la dematerializzazione dei flussi documentali relativi ai principali procedimenti amministrativi dell'Ufficio, attraverso la prosecuzione dello sviluppo della piattaforma @Doc (già operativa per il Ministero degli affari esteri-Mae attraverso Cineca) e della collaborazione tecnica con il Ministero degli affari esteri, conformemente all'accordo sottoscritto in data 11 novembre 2011 dall'Autorità e dal Ministero stesso; all'interno di tale rapporto di collaborazione si situa il progetto (in fase di realizzazione) di *workflow* dei flussi documentali.

Riguardo all'attività di carattere economale, la maggior parte degli interventi ha riguardato la manutenzione ordinaria e straordinaria degli impianti e la gestione logistica degli interventi straordinari che la società proprietaria dell'immobile ha eseguito sullo stesso.

Riguardo alla logistica, si segnala lo scarto di materiale avvenuto nel febbraio 2014, che ha in buona parte risolto i problemi di accumulo di documentazione superata e di beni in disuso, con conseguente liberazione di spazi utili alle varie articolazioni dell'Ufficio. In particolare, il materiale cartaceo è stato individuato da apposita Commissione, ai sensi della normativa vigente in materia di scarto d'atti d'archivio.

L'Autorità, sulla base di un apposito studio e di opportuni approfondimenti effettuati dal Dipartimento contratti e risorse finanziarie, ha poi provveduto a dismettere una porzione dell'immobile (adibita a Sala Conferenze e Biblioteca) con un risparmio previsto pari a circa il 13% della spesa di locazione. La procedura di dismissione, che è stata curata tenendo conto delle necessità dell'Ufficio e gestita secondo i criteri di efficienza ed economicità, si è conclusa per la parte logistica a dicembre 2014. A seguito di asta pubblica andata deserta, si è provveduto anche alla cessione a titolo gratuito di alcuni beni mobili inerenti la Sala Conferenze a due enti pubblici, per mezzo di un'apposita procedura comparativa. Il patrimonio librario è stato riallocato, dopo attenta valutazione riguardante anche la fattibilità in termini di sicurezza, in altri locali dell'Autorità riutilizzando il mobilio preesistente (cfr. par. 24.9).

Da ultimo, è proseguita, rispetto all'anno precedente, l'attività di aggiornamento e "formazione" curata dal Dipartimento competente nei confronti degli altri dirigenti/funzionari che, in relazione a specifici appalti, potrebbero essere designati quali Rup, contribuendo allo svolgimento delle numerose funzioni richieste a tale figura nel pieno rispetto della vigente normativa. Particolare attenzione è stata prestata alle novità normative, anche sotto il profilo delle procedure di gara, quali l'introduzione del cd. sistema AVCPass.

25.3. *Le novità legislative e regolamentari e l'organizzazione dell'Ufficio*

È proseguita la rigorosa attuazione delle disposizioni previste dal d.l. 31 maggio 2010, n. 78, convertito, con modificazioni, dalla l. 30 luglio 2010, n. 122. In tale quadro, anche nel periodo considerato, non sono stati conferiti incarichi di consulenza e, quanto alle auto di servizio, l'Autorità continua a disporre esclusivamente della sola vettura di servizio messa a disposizione dalla Guardia di finanza ed utilizzata per le esigenze di mobilità del Presidente (cfr. par. 25.1).

L'art. 22, d.l. 24 giugno 2014, n. 90, convertito con modificazioni nella l. 11 agosto 2014, n. 114, ha introdotto significative novità per l'Autorità alle quali si è iniziato a dar corso nell'anno in considerazione. Come si è detto (par. 25.2), è stata stipulata con l'Autorità per l'energia elettrica, il gas e il sistema idrico e l'Autorità per le garanzie nelle comunicazioni, una convenzione per la gestione in modo unitario di alcuni servizi strumentali. È stata inoltre aperta alla firma di tutte le autorità indipendenti, la convenzione per la gestione unitaria delle procedure concorsuali per il reclutamento di personale. Il medesimo articolo ha altresì previsto, al comma 5, una riduzione almeno pari al 20% delle retribuzioni accessorie del personale delle autorità: in merito, attesa la diversità di situazioni fra i vari organismi e la non univoca individuazione del trattamento di carattere accessorio, è stato avviato un importante lavoro di approfondimento, anche in collaborazione con altre autorità. Nelle more, onde non pregiudicare gli effetti della manovra e non ritardarne l'applicazione, è stato adottato un provvedimento provvisorio che ha inciso nella misura del 20% sulla retribuzione di risultato e sul lavoro straordinario dei dipendenti.

Con riferimento alle politiche del personale, pur nel contesto di una sensibile riduzione dello stanziamento a disposizione dell'Autorità (par. 25.1), è stata dispiegata ogni possibile iniziativa per potenziarne l'organico, elemento indispensabile al fine di poter far adeguatamente fronte alle accresciute esigenze dell'attività istituzionale.

Nel 2014, quindi, a seguito di apposita procedura di mobilità volontaria esterna, ai sensi dell'art. 30, d.lgs. n. 165/2001, conclusasi nel 2013, sono stati immessi in ruolo due funzionari con profilo informatico/tecnologico ed è stata portata a compimento l'analoga procedura avviata per la ricerca di funzionari con profilo giuridico con l'immissione in ruolo di un funzionario risultato in possesso dei requisiti richiesti.

La legge 27 dicembre 2013, n. 147 (legge di stabilità 2014), all'art. 1, commi 268 e 269, ha poi comportato novità di rilievo per l'Autorità: essa ha infatti stabilito, 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, un incremento della consistenza del personale dell'organico del Garante 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 tali finalità, il Garante è stato autorizzato a indire una o più procedure concorsuali per assunzioni a tempo indeterminato di personale in servizio presso l'Ufficio, alla data di entrata in vigore della citata legge di stabilità, con contratto a tempo determinato che, alla data di pubblicazione del relativo bando, avesse maturato almeno tre anni di anzianità con contratto a tempo determinato. Tali disposizioni, non prevedevano oneri aggiuntivi a carico delle finanza pubblica, collocandosi nel solco di quanto previsto per le amministrazioni pubbliche dall'art. 4, comma 6, d.l. 31 agosto 2013, n. 101, convertito, con modificazioni, dalla l. 30 ottobre 2013, n. 125, consentendo un rafforzamento dell'organico e, nel contempo, una valorizzazione di professionalità che altrimenti sarebbero andate disperse. Come si dirà in seguito, nel corso del 2014 sono state espletate pertanto due procedure concorsuali per l'assunzione con contratto a tempo indeterminato di personale avente i requisiti sopracitati.

Forte impulso è stato dato all'attività formativa del personale. In particolare, è stata predisposta una bozza delle linee guida in materia di formazione, approvata in prima lettura dal Collegio ed inoltrata alle OO.SS. Inoltre, come si dirà nel prossimo paragrafo, un elevato numero di dipendenti ha partecipato a corsi di formazione in materie di particolare interesse dell'Autorità.

Servizio di segreteria del Collegio

All'interno dell'Autorità il Servizio di segreteria del Collegio ha curato gli adempimenti necessari allo svolgimento delle attività di tale organo (predisposizione e distribuzione della documentazione necessaria per le riunioni del Collegio, conservazione dei verbali delle riunioni e degli originali delle deliberazioni adottate e del materiale utile per la pubblicazione in GU); ha provveduto inoltre, in stretto raccordo con le diverse articolazioni dell'Ufficio, al controllo dei testi deliberati dal Collegio e destinati – tramite la redazione web – alla pubblicazione sul sito istituzionale dell'Autorità.

Conformemente a quanto disposto dall'art. 15 del Regolamento n. 1/2000 e nel rispetto del Cad, l'Autorità ha proseguito nell'utilizzo di modalità di trasmissione elettronica dei documenti predisposti per l'esame e l'approvazione da parte del Collegio, per assicurare maggiore celerità ed efficienza nonché la progressiva sostituzione del mezzo cartaceo con quello elettronico, con risparmio di costi e tempo nonché recupero di spazio.

Si segnala anche la piena fruibilità, nell'area intranet, dei testi dei provvedimenti adottati dal Collegio, per i quali dal 2011 è stato improntato l'apposito registro interno delle deliberazioni collegiali.

Mediante il Servizio di segreteria sono altresì gestite eventuali richieste di oscuramento dei dati identificativi pervenute all'Ufficio da parte degli interessati o dai titolari del trattamento contenute nei provvedimenti del Garante.

25.4. *Il personale e i collaboratori esterni*

Nel 2014, a conclusione della procedura di mobilità volontaria esterna per funzionario con profilo giuridico, indetta ai sensi dell'art. 30, d.lgs. n. 165/2001, è stato dichiarato idoneo a ricoprire la relativa posizione, ed immesso nel ruolo organico, un funzionario appartenente ad altra amministrazione pubblica; sono stati immessi inoltre, nel ruolo organico, due funzionari con profilo informatico/tecnologico, a seguito di analoga procedura di mobilità esterna conclusa nel 2013.

L'Autorità ha poi dato attuazione all'art. 1, commi 268 e 269, l. 27 dicembre 2013, n. 147 (legge di stabilità 2014), la quale, al fine di non disperdere la professionalità acquisita dal personale con contratto a tempo determinato, assunto a seguito di procedura selettiva pubblica, ha previsto la possibilità di indire, entro il 31 dicembre 2016, una o più procedure concorsuali per assunzioni a tempo indeterminato di personale in servizio presso l'Ufficio che, alla data di pubblicazione del relativo bando, avesse maturato almeno tre anni di anzianità con contratto a tempo determinato. A tal fine, sono state indette due procedure concorsuali, con la conseguente immissione in ruolo di un dirigente amministrativo-contabile e nove funzionari.

Nelle more dell'espletamento delle suddette procedure concorsuali, sono stati rinnovati cinque contratti 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.

Nel 2014, sono cessate a vario titolo dal servizio presso il Garante, n. 4 unità di personale in posizione di comando o fuori ruolo, di cui due con qualifica di dirigente e due di funzionario; una unità del ruolo organico con la qualifica di dirigente è stata collocata in quiescenza.

Nel periodo di riferimento si sono svolte due procedure per la selezione di giovani laureati per l'effettuazione di periodi di tirocinio e sette giovani laureati hanno svolto un periodo di formazione e orientamento presso l'Autorità.

Al 31 dicembre 2014 l'Ufficio poteva contare centoventicinque unità previste in organico (cfr. sez. IV, tab. 22), di cui centododici in servizio, al quale va aggiunto un contingente di personale a contratto di otto unità (cfr. sez. IV, tab. 23).

Dai suddetti dati emerge un incremento di otto unità di personale in servizio rispetto all'anno precedente e la contestuale riduzione, nella misura di dieci unità, del contingente dei contratti a tempo determinato, in attuazione del citato art. 1, commi 268 e 269, l. n. 147/2013 (legge di stabilità 2014).

Particolare attenzione è stata riservata alla formazione del personale. Nel corso dell'anno è proseguita, nell'ambito di una convenzione a suo tempo stipulata tra il Garante e la Ssef (Scuola superiore dell'economia e delle finanze), la partecipazione di un elevato numero di dipendenti ai corsi organizzati dalla predetta Scuola; sono stati tenuti, inoltre, da varie unità organizzative dell'Ufficio, diversi seminari formativi interni, su temi di particolare interesse per l'attività del Garante.

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 Presidenza del Consiglio dei ministri e della Ragioneria generale dello Stato.

25.5. *Il settore informatico e tecnologico*

Sistema informativo e servizi ICT

È proseguita l'attività di sviluppo del sistema informativo nel solco delle direttrici di innovazione tracciate dal Codice dell'amministrazione digitale (Cad), accentuando la smaterializzazione dei flussi documentali e la cooperazione interna.

Tra gli interventi più significativi si citano, nell'ambito del progetto di automazione dei flussi documentali basato sul sistema @doc acquisito in riuso dal Ministero degli affari esteri e sulla piattaforma documentale Alfresco, la messa a punto dei *test* relativi al flusso "Ricorsi", l'analisi e i primi sviluppi relativi ai flussi "Schema di provvedimento" e "Adunanza collegiale".

Inoltre sono stati realizzati diversi interventi di aggiornamento dei sistemi informativi, tra cui: la messa in opera di un nuovo sistema di produzione della rassegna stampa; la creazione e il popolamento iniziale del nuovo registro di protocollo per atti e delibere del segretario generale; le nuove funzionalità del sito web istituzionale, con l'introduzione di funzionalità vocali per l'ascolto dei testi *online* e di strumenti per la deindicizzazione dei contenuti del sito da parte dei motori di ricerca.

Per quanto riguarda gli aspetti infrastrutturali, è stato attivato un collegamento in fibra ottica di tipo *Wavelength Division Multiplexing* tra il Garante e il *datacenter* del Consorzio Cineca che garantisce un'ampiezza di banda internet fino 1 Gbps, ovvero 50 volte superiore al precedente collegamento, fornendo in aggiunta, su una differente lunghezza d'onda, una capacità trasmissiva di ben 4 Gbps gestita in tecnologia *Fibre Channel* per la realizzazione di procedure di *disaster recovery* e di salvataggio remoto dei dati. In coincidenza con l'attivazione del nuovo *link* Ip sono stati introdotti nuovi apparati *firewall* che fungono anche da punto di accesso Vpn (*Virtual private network*).

Le procedure di salvataggio automatico dei dati sono state aggiornate con la configurazione dei *backup* mediante il *software* Avamar e l'installazione di una nuova *tape library* per il riversamento locale dei *backup* su nastro magnetico.

È stato completato il progetto della nuova carta multifunzione dell'Autorità, con il rilascio agli utenti di tessere *smartcard* di tipo Cns (Carta nazionale dei servizi)

arricchite con funzionalità di *smart logon* tramite i certificati di autenticazione Cns, di rilevamento a radiofrequenza (Rfid) e dotate di caratteristiche funzionali al riconoscimento a vista.

È stata realizzata una nuova architettura per la gestione della posta elettronica in ingresso e in uscita dal dominio "gpdp.it", utilizzando un nuovo *mail gateway* dotato di capacità avanzate di rilevamento di *malware* a protezione delle comunicazioni elettroniche e dei dati.

Sicurezza informatica dell'Ufficio

Nessun evento relativo alla sicurezza ha prodotto danni o disservizi nel dominio dell'Ufficio. Si è registrato un unico incidente informatico di rilievo, con un guasto di molteplicità 2 a un sottosistema di *storage* prodottosi in orario notturno e sviluppatosi nel corso di giornate non lavorative, che è stato affrontato con interventi straordinari di manutenzione e con il ripristino dei dati a partire da copie di sicurezza, con impatto sulla disponibilità dei dati interessati dal guasto limitato a poche ore.

IV - I dati statistici 2014

Sintesi delle principali attività dell'Autorità	
Numero complessivo dei provvedimenti collegiali adottati	628
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
Autorizzazioni individuali al trattamento dei dati sensibili e giudiziari (art. 41 del Codice)	2
Provvedimenti concernenti trasferimenti di dati consentiti verso Paesi terzi (art. 44, comma 1, lett. *a*), del Codice)	9
Altri provvedimenti del Garante (artt. 10, comma 2, 13, comma 5, lett. *c*), 150, comma 5, del Codice)	9
Decisioni su ricorso (art. 145 del Codice)	306
Provvedimenti collegiali su segnalazioni e reclami (artt. 142-144 del Codice) nonché a seguito di accertamenti d'ufficio (art. 154 del Codice)	87
Ordinanze-ingiunzione adottate dal Garante	142
Riscontri a segnalazioni, reclami, richieste di parere e quesiti (artt. 142-144 del Codice e artt. 5 e 11, Reg. Garante n. 1/2007)	4.894
Provvedimenti collegiali su verifiche preliminari per trattamenti che presentano rischi specifici (art. 17 del Codice)	15
Provvedimenti a seguito di comunicazione al Garante di flussi di dati tra p.a. o in materia di ricerca scientifica (artt. 19, comma 3, 39 e 110 del Codice)	8
Pareri a soggetti pubblici sul trattamento dei dati sensibili e giudiziari	13
Risposte ad atti di sindacato ispettivo e di controllo	9
Risposte a quesiti e altre istanze	33.201
Rilievi formulati in relazione a leggi regionali ai fini dell'impugnazione ex art. 127 Cost.	1
Accertamenti e controlli efffettuati *in loco* (artt. 157-158 del Codice)	385
Violazioni amministrative contestate	577
Sanzioni applicate con ordinanza di ingiunzione	202
Pagamenti derivanti dall'attività sanzionatoria	€4.907.866
Comunicazioni di notizia di reato all'autorità giudiziaria	39
Prescrizioni sulle misure minime di sicurezza (a fini di estinzione del reato)	4
Ricorsi (trattati) *ex* art. 152 del Codice	31
Opposizioni (trattate) a provvedimenti del Garante	80
Notificazioni pervenute nell'anno 2014	1.392
Notificazioni pervenute dal 2004 al 31 dicembre 2014	24.075
Riunioni del Gruppo Art. 29	5
Partecipazione a sottogruppi di lavoro - Gruppo Art. 29	22
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	29
Quesiti, questionari e richieste di contributi provenienti da altre Autorità e Istituzioni	53

Tabella 1. Sintesi delle principali attività dell'Autorità

Attività di comunicazione dell'Autorità	
Comunicati stampa	48
Newsletter	15
Dvd (archivio digitale su normativa italiana e attività del Garante)	2
Prodotti editoriali	3
Video divulgativi	1
Schede informative	5

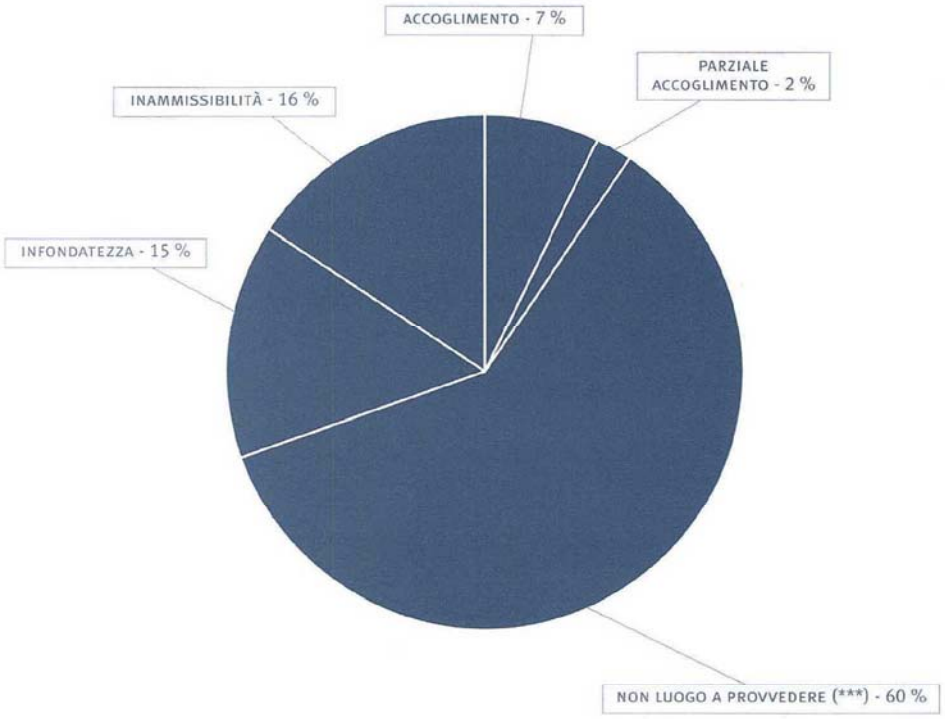
Tabella 2. Attività di comunicazione dell'Autorità

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
Processo telematico	2
Informatizzazione e banche dati della p.a.	11
Formazione	2
Attività produttive e professioni	1
Esercizio dei diritti	2
Trattamento dati sensibili e giudiziari	2
Totale	**22**

Tabella 4. Tipologia delle decisioni su ricorsi

Decisioni su ricorsi	
Tipi di decisione (**)	**Numero ricorsi**
Accoglimento	22
Parziale accoglimento	7
Non luogo a provvedere (***)	184
Infondatezza	45
Inammissibilità	48
Totale	**306**



(*) Inerenti anche ad affari pervenuti anteriormente al 2014
(**) Le decisioni sui ricorsi possono contenere più statuizioni in base alle diverse richieste presentate: la statistica prende in esame, in tali casi, la statuizione più "favorevole" al ricorrente
(***) Casi nei quali le richieste del ricorrente sono state soddisfatte nel corso del procedimento

Categorie di titolari	Numero ricorsi
Banche e società finanziarie	80
Compagnie di assicurazione	10
Sistemi di informazioni creditizie	28
Società di informazioni commerciali	9
Amministrazioni pubbliche e concessionari di pubblici servizi	3
Strutture sanitarie pubbliche e private	8
Parrocchie	2
Fornitori telefonici e telematici	24
Attività di *marketing* svolta da imprenditori privati	31
Datori di lavoro pubblici e privati	39
Editori (anche televisivi)	42
Liberi professionisti	7
Amministrazioni condominiali	5
Altri	18
Totale	**306**

Tabella 5. Suddivisione dei ricorsi in relazione alle categorie di titolari del trattamento

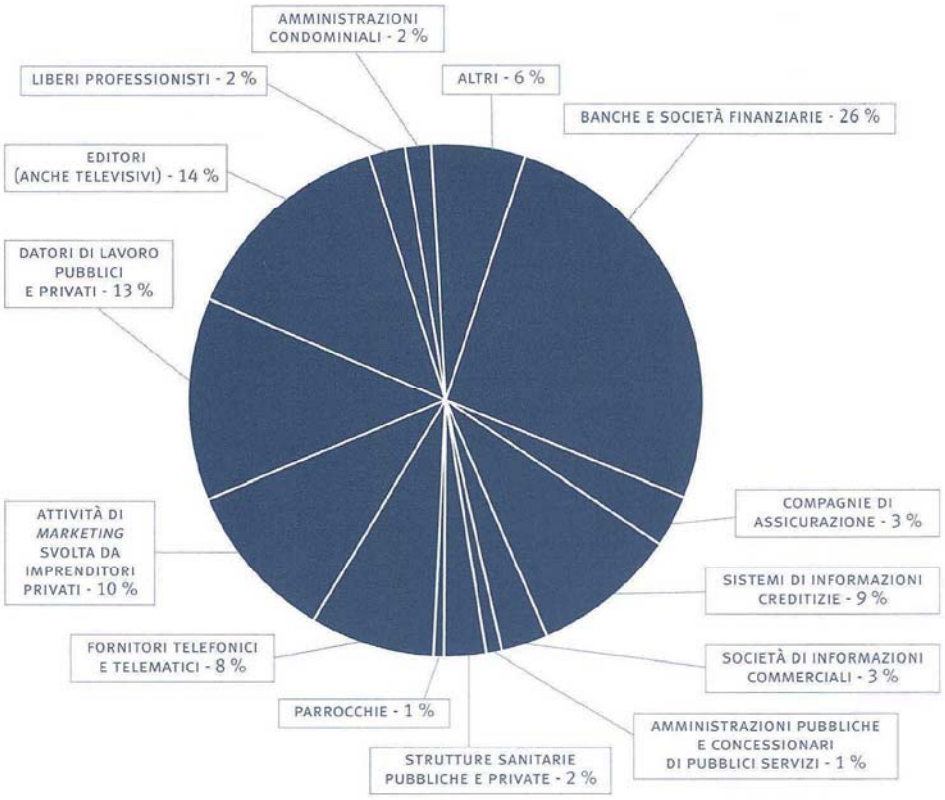
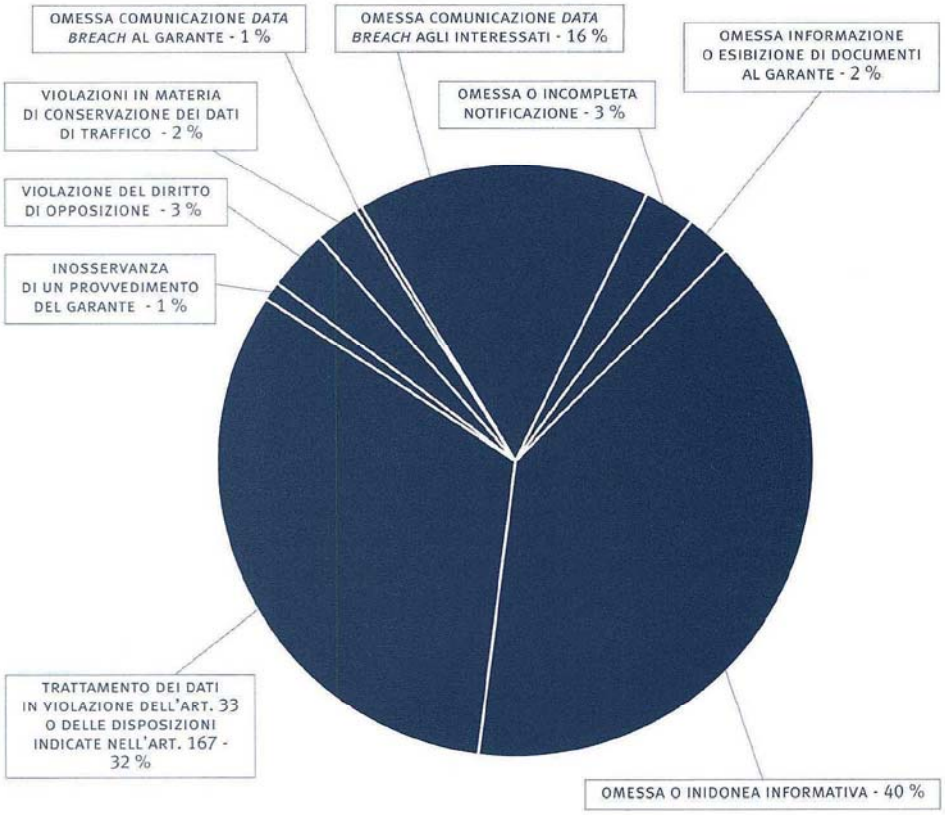


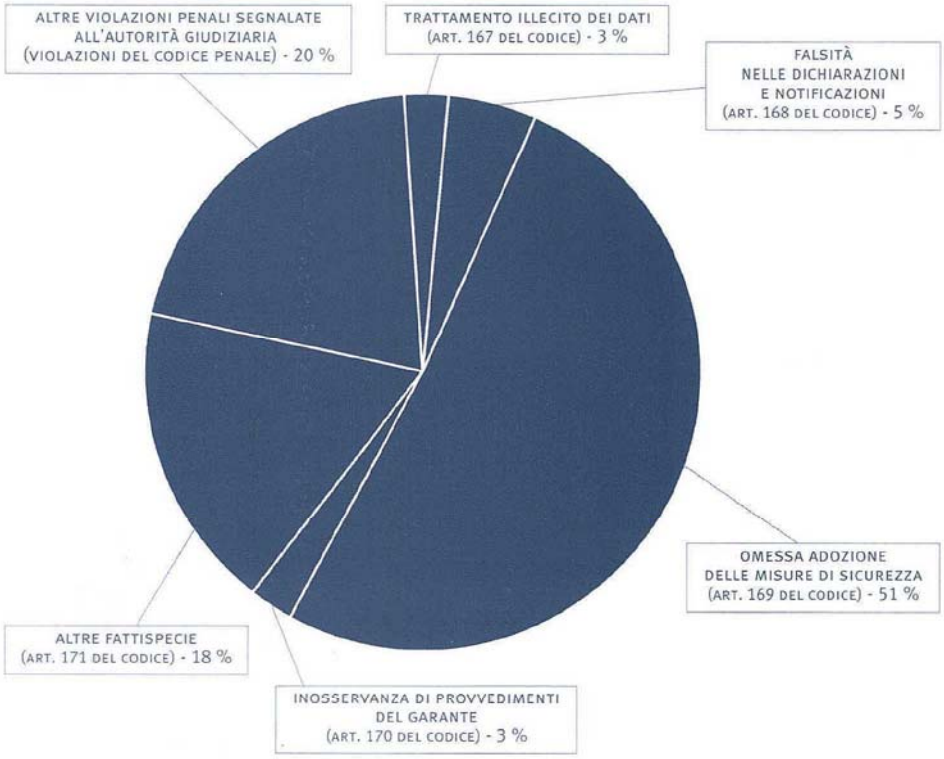
Tabella 6. Violazioni amministrative contestate

Violazioni amministrative contestate	
Omessa o inidonea informativa (art. 161 del Codice)	228
Trattamento dei dati in violazione dell'art. 33 o delle disposizioni indicate nell'art. 167 (art. 162, comma 2-*bis*, del Codice)	186
Inosservanza di un provvedimento del Garante (art. 162, comma 2-*ter*, del Codice)	6
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)	14
Omessa comunicazione di eventi di *data breach* al Garante (art. 162-*ter*, comma 1 del Codice)	2
Omessa comunicazione di eventi di *data breach* agli interessati (art. 162-*ter*, comma 2 del Codice)	92
Omessa o incompleta notificazione (art. 163 del Codice)	16
Omessa informazione o esibizione di documenti al Garante (art. 164 del Codice)	14
Totale	577



Comunicazioni di notizia di reato all'autorità giudiziaria	
	Segnalazioni
Trattamento illecito dei dati (art. 167 del Codice)	1
Falsità nelle dichiarazioni e notificazioni (art. 168 del Codice)	2
Omessa adozione delle misure di sicurezza (art. 169 del Codice)	20
Inosservanza di provvedimenti del Garante (art. 170 del Codice)	1
Altre fattispecie (art. 171 del Codice)	7
Altre violazioni penali segnalate all'autorità giudiziaria (violazioni del codice penale)	8
Totale	39

Tabella 7. Comunicazioni di notizia di reato all'autorità giudiziaria



Pagamenti derivanti dall'attività sanzionatoria	
Somme versate a titolo di oblazione in via breve	2.374.135
Somme versate in conseguenza di ordinanze ingiunzione	1.968.136
Ammontare complessivo delle somme pagate in sede di "ravvedimento operoso" (art. 169 del Codice)	120.000
Ulteriori entrate derivanti dall'attività sanzionatoria	445.595
Totale	4.907.866

Tabella 8. Pagamenti derivanti dall'attività sanzionatoria

Quesiti		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale quesiti	272	401

Tabella 9. Quesiti

(*) Inerenti anche ad affari pervenuti anteriormente al 2014

Tabella 10. Segnalazioni e reclami

Segnalazioni e reclami		
	Pervenuti nell'anno	Riscontri resi nell'anno (*)
N. totale segnalazioni e reclami	**4.170**	**4.493**
Temi principali		
Assicurazioni	68	81
Associazioni	45	46
Centrali rischi	102	143
Concessionari pubblici servizi	57	73
Condominio	40	56
Credito	275	459
Data breach	19	13
Enti locali	113	113
Giornalismo e libertà d'espressione	95	98
Imprese	95	116
Informazioni commerciali	3	22
Internet	74	85
Istruzione	59	59
Lavoro	240	137
Marketing (posta cartacea, *e-mail*, fax, sms)	160	165
Marketing telefonico	2.220	1.410
Recupero crediti	124	98
Sanità e servizi di assistenza sociale	92	92
Videosorveglianza	174	176

Tabella 11. Atti di sindacato ispettivo e controllo

Atti di sindacato ispettivo e controllo	
Temi	Numero
Trattamento dei dati da parte dei *social network*	1
Programma PRISM della *National Security Agency* statunitense (NSA)	1
Esercizio dei diritti	1
Accordo commerciale internazionale di partenariato transatlantico per il commercio e gli investimenti (TTIP)	3
Trattamento di dati personali nell'attività di promozione commerciale svolta mediante *call center*	2
Cyberbullismo	1
Totale	**9**

Tabella 12. Tipologie di notificazioni pervenute nel periodo 2004-2014

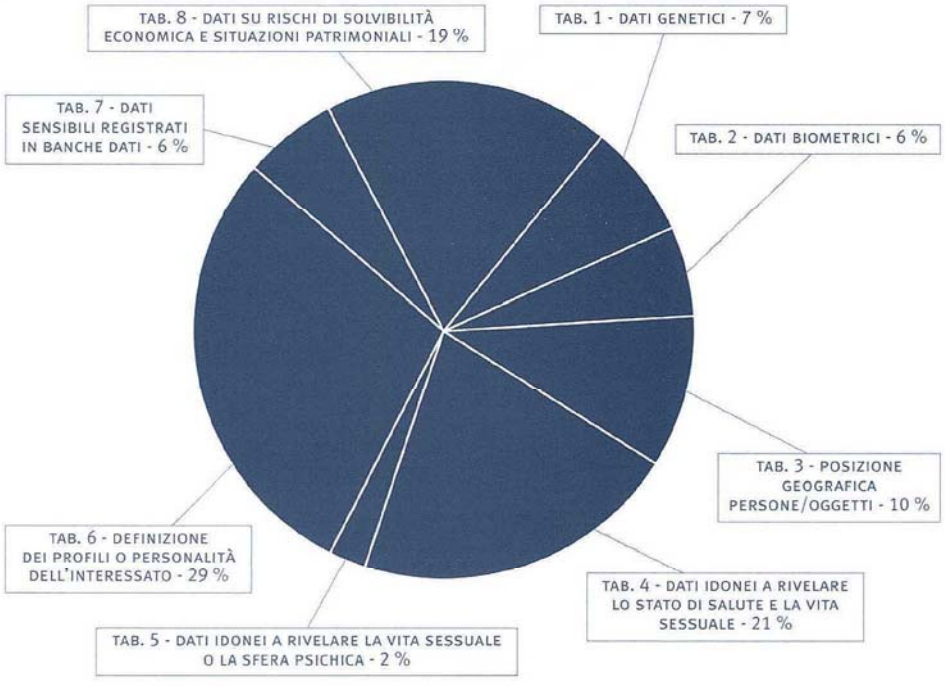
Tipologie di notificazioni pervenute nel periodo 2004-2014 (**)			
	Da soggetti pubblici	Da soggetti privati	Totale pervenute (**)
Prima notificazione al Garante	1.211	18.164	19.375
Modifica di una precedente notificazione	153	3.548	3.701
Notificazione della cessazione del trattamento	73	926	999
Totale	**1.437**	**22.638**	**24.075**

(*) Inerenti anche ad affari pervenuti anteriormente al 2014

(**) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2014

Suddivisione delle notificazioni per tipologia di trattamento effettuato: 2004-2014	
Tabelle di notificazione compilate (*)	Numero
Tabella 1 - Trattamento di dati genetici	2.632
Tabella 2 - Trattamento di dati biometrici	2.050
Tabella 3 - Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica	3.528
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	7.497
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	846
Tabella 6 - Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con l'esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi	10.245
Tabella 7 - Trattamento di dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie	2.142
Tabella 8 - Trattamento di dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti	6.548
Totale (**)	**35.488**

Tabella 13. Suddivisione delle notificazioni per tipologia di trattamento effettuato: 2004-2014



(*) Situazione alla data del 31 dicembre 2014
(**) N.B. Il totale è superiore alla sommatoria delle precedenti tabelle in quanto una singola notificazione può riguardare più trattamenti

Tabella 14. Evoluzione su base annua delle tipologie di trattamento notificate al Garante dal 2004 al 2014

Tabella del registro dei trattamenti												
	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	Totali al 31.12.14
Dati genetici (tab. 1)	1.250	226	282	84	110	94	134	131	78	103	140	2.632
Dati biometrici (tab. 2)	808	155	218	73	121	103	106	78	59	130	199	2.050
Dati idonei ad indicare la posizione geografica di persone od oggetti (tab. 3)	1.160	241	316	116	139	211	165	220	243	313	404	3.528
Dati idonei a rivelare lo stato di salute o la vita sessuale (tab. 4)	3.669	585	855	249	255	197	396	381	320	292	298	7.497
Dati idonei a rivelare la vita sessuale o la sfera psichica (tab. 5)	435	84	117	22	30	28	33	32	18	20	27	846
Dati idonei a definire il profilo o la personalità dell'interessato (tab. 6)	3.582	778	728	481	684	478	641	658	543	918	754	10.245
Dati sensibili per fini di selezione o per ricerche di mercato (tab. 7)	1.010	185	218	101	92	83	80	97	63	97	116	2.142
Dati relativi a rischi di solvibilità economica e di frode (tab. 8)	3.170	450	619	255	435	283	256	250	181	305	344	6.548
Totali	15.084	2.704	3.353	1.381	1.866	1.477	1.811	1.847	1.505	2.178	2.282	35.488

Grafico 15. Tipologie di trattamento notificate - Evoluzione dal 2005 al 2014

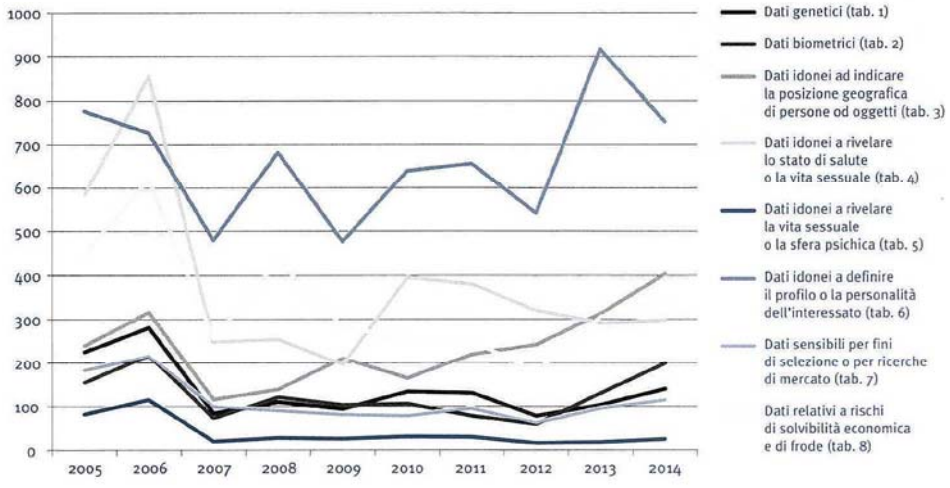


Tabella 16. Raffronto tipologie di trattamento notificate - Anni 2004 e 2014

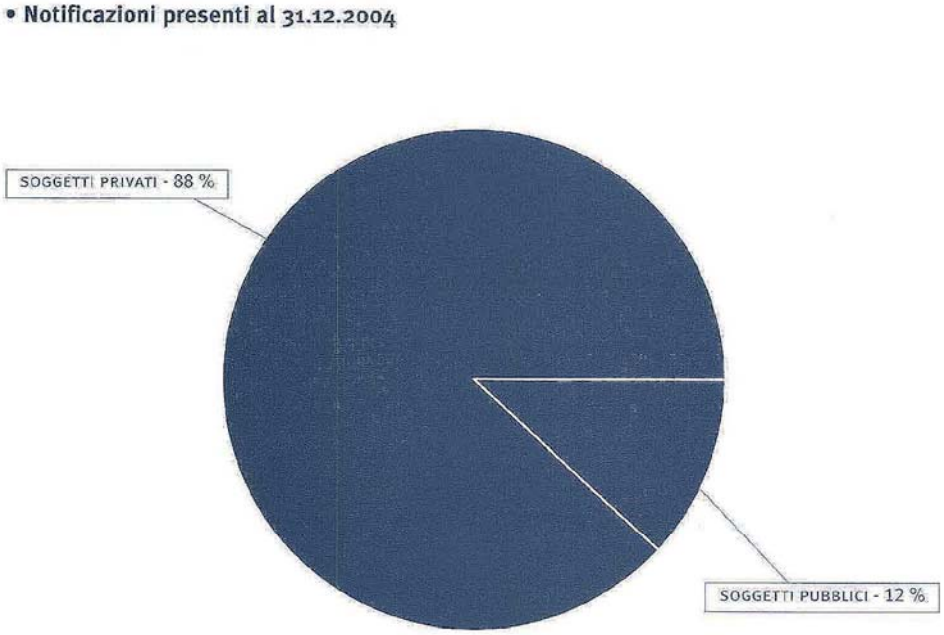
Tipologie di trattamento	31.12.2004		31.12.2014	
	N. tabelle compilate	% sul totale	N. tabelle compilate	% sul totale
Trattamento di dati genetici (tab. 1)	1.250	8,3%	2.632	7,4%
Trattamento di dati biometrici (tab. 2)	808	5,4%	2.050	5,8%
Trattamento di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica (tab. 3)	1.160	7,7%	3.528	9,9%
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 (tab. 4)	3.669	24,3%	7.497	21,1%
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 (tab. 5)	435	2,9%	846	2,4%
Trattamento effettuato con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con l'esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi (tab. 6)	3.582	23,7%	10.245	28,9%
Trattamento di dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie (tab. 7)	1.010	6,7%	2.142	6%
Trattamento di dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti (tab. 8)	3.170	21%	6.548	18,5%
Totale	**15.084**	**100%**	**35.488**	**100%**

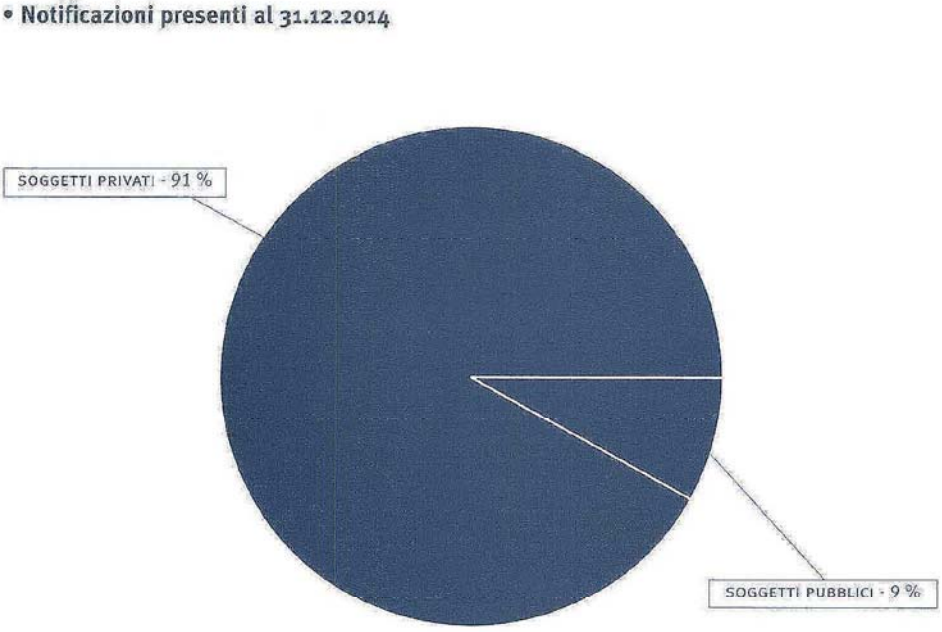
Tabella 17. Tipologie di notificazioni pervenute nel 2014

Tipologie di notificazioni pervenute nel 2014 (*)	Da soggetti pubblici	Da soggetti privati	Totale pervenute (*)
Prima notificazione al Garante	28	961	989
Modifica di una precedente notificazione	17	317	334
Notificazione della cessazione del trattamento	1	68	69
Totale	**46**	**1346**	**1392**

(*) In tutte le tabelle i valori sono riferiti alla data del 31 dicembre 2014

Grafico 18. Raffronto delle notificazioni presenti sul registro dei trattamenti per gli anni 2004 e 2014 in base alla natura pubblica/privata del titolare del trattamento





• **Trattamenti notificati da soggetti pubblici al 31.12.2014**

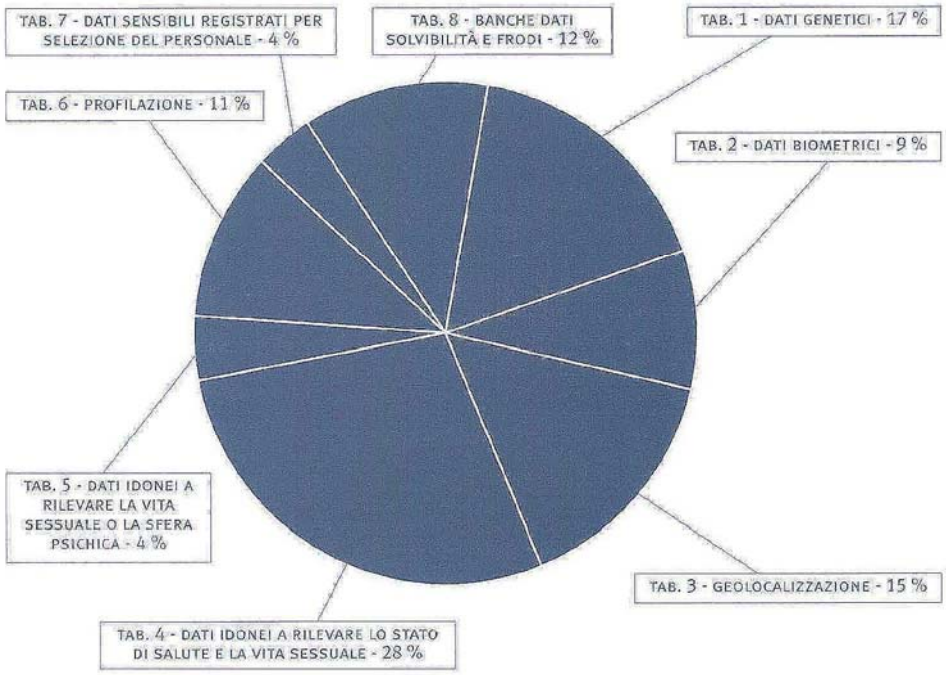


Grafico 19. Raffronto della composizione delle tipologie di trattamento notificate al 31.12.2014 in base alla natura pubblica/ privata del titolare del trattamento

• **Trattamenti notificati da soggetti privati al 31.12.2014**

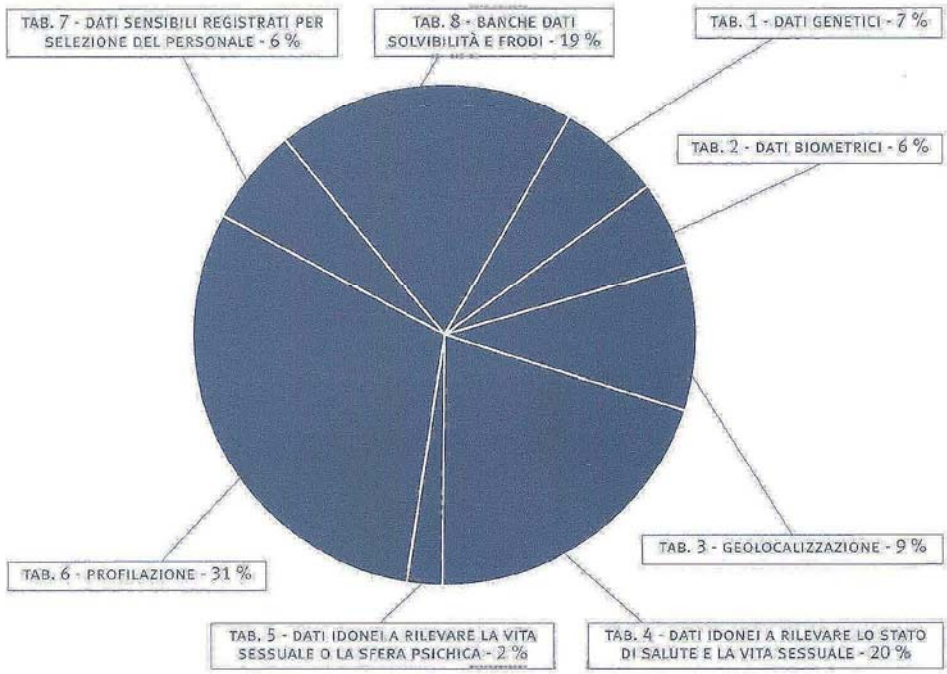


Tabella 20. Ufficio relazioni con il pubblico

Ufficio relazioni con il pubblico	
	2014
E-mail esaminate	18.717
Contatti telefonici	13.525
Persone in visita all'Urp	363
Trattazione fascicoli	596
Totale	**33.201**

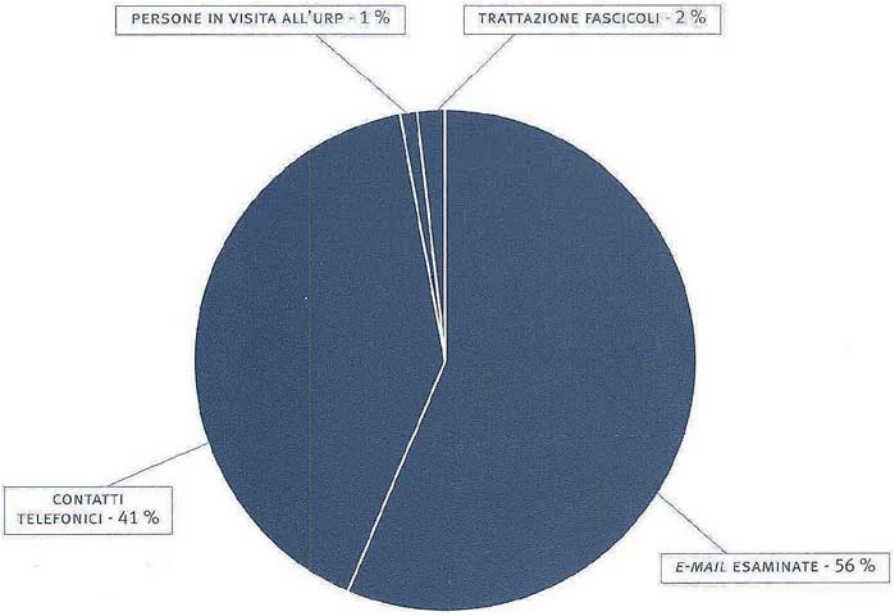


Grafico 21. *E-mail* esaminate dall'Ufficio relazioni con il pubblico

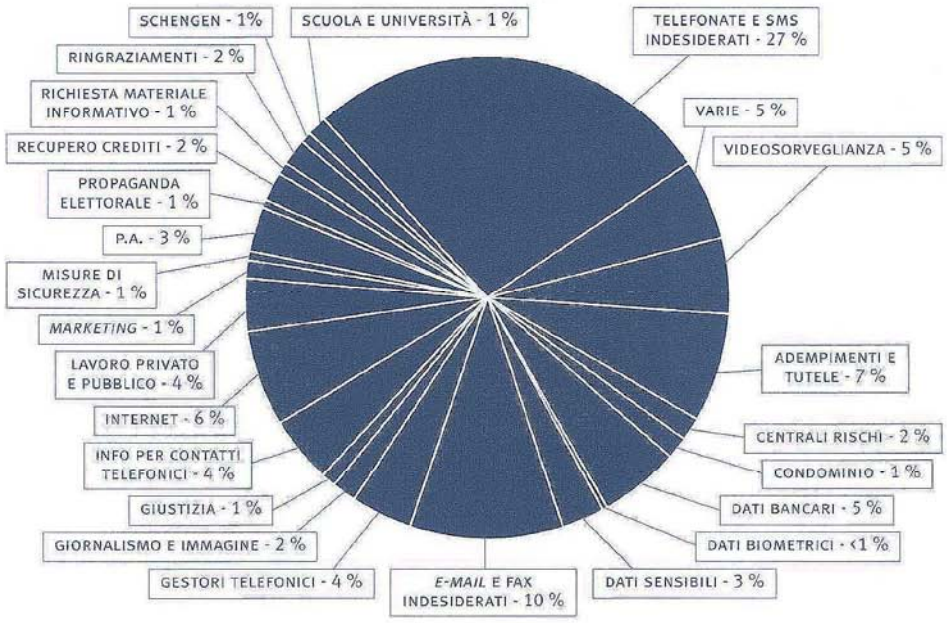


Tabella 22. Posti previsti in organico

Posti previsti in organico	
Segretario generale	1
Dirigenti	24
Funzionari	69
Operativi	30
Esecutivi	1
Totale	125
Personale a contratto	20

Tabella 23. Personale in servizio

Personale in servizio (*)				
Area	In ruolo (a)	In posizione di fuori ruolo (b)	Comandato presso altre amministrazioni o in aspettativa (c)	Impiegato dall'Ufficio (a+b-c)
Segretario generale	1	–	–	1
Dirigenti	14	2	1	15
Funzionari	73	2	3	72
Operativi	25	–	1	24
Esecutivi	–	–	–	–
Totali	**113**	4	5	**112**
Personale a contratto				8

Tabella 24. Risorse finanziarie

Risorse finanziarie						
Entrate accertate	**Anno 2014**		**Anno 2013**		**Differenza**	
Entrate correnti		20.969.494		23.029.146		-2.059.652
di cui trasferimento dallo Stato	7.621.271		8.379.264		-757.993	
Totale entrate		**20.969.494**		**23.029.146**		**-2.059.652**
Spese impegnate	**Anno 2014**		**Anno 2013**		**Differenza**	
Spese di funzionamento		18.048.088		18.389.709		-341.621
Spese in conto capitale		374.020		26.992		347.028
Rimborsi al Mef e transazioni		673.612		253.611		420.001
Totale spese		**19.095.720**		**18.670.312**		**425.408**

(*) Situazione alla data del 31 dicembre 2014

Tabella 25. Attività internazionali dell'Autorità

Unione europea			
Gruppo Articolo 29	**Sessione plenaria Art. 29**		26 e 27 febbraio 9 e 10 aprile 3 e 4 giugno 16 e 17 settembre 25 e 26 novembre
	Riunioni dei sottogruppi	*Border Travel Law Enforcement* (BTLE)	14 gennaio 6 febbraio 20 marzo 15 maggio 26 agosto 4 novembre
		E-Government	6 febbraio 13 novembre
		Financial Matters	27 agosto 5 novembre
		Future of Privacy	4 aprile 15 luglio 8 ottobre 14 novembre
		International Transfers	10 gennaio (*conference call*) 6 maggio 17 luglio 23 ottobre
		Technology	15 e 16 gennaio 18 e 19 marzo 13 e 14 maggio 21 e 22 ottobre

Unione europea	
Autorità di controllo comune EUROPOL	3/7 marzo, Ispezione 19 marzo 27 e 28 maggio, "Europol e New Project Group" 16 giugno 2 ottobre 24 e 25 novembre, Europol e sottogruppo "Europol New Project Group" 9 dicembre
Gruppo di coordinamento della supervisione IMI	6 maggio
Autorità di controllo comune DOGANE	17 giugno 10 dicembre
Gruppo di coordinamento della supervisione SID	17 giugno 10 dicembre
Gruppo di coordinamento della supervisione SIS II	8 maggio 28 ottobre
Gruppo di coordinamento della supervisione EURODAC	7 maggio 29 ottobre
Gruppo di coordinamento della supervisione VIS	7 maggio 29 ottobre

Unione europea		
Riunioni di gruppi di esperti	**Consiglio UE - Dapix (Regolamento)**	8, 9 e 10 gennaio 20 e 21 gennaio 5 e 6 febbraio 18, 19 e 20 febbraio 12 e 13 marzo 7 e 8 maggio 15 e 16 maggio 10 e 11 luglio 11 e 12 settembre 30 settembre e 1° ottobre 21 e 22 ottobre 28 ottobre 6 e 7 novembre 12 novembre 20 e 21 novembre 17 dicembre
	Consiglio UE - Dapix (Direttiva)	27 gennaio 26 febbraio 24 marzo 19 maggio 27 ottobre 24 novembre
	Consiglio UE - *Friends of Presidency*	1° ottobre
	Commissione UE - *Data retention*	14 marzo 11 aprile
Commissione UE - *Meeting* sull'uso civile dei droni		28 febbraio
Commissione UE - *Data breach notifications under the e-Privacy Directive*		11 marzo 12-13 giugno 10 dicembre

Altri *forum* internazionali		
Organizzazione per la cooperazione e lo sviluppo economico (OCSE)	Comitato *"Working Party on Security and Privacy in the Digital Economy"*	21 marzo (*ad hoc meeting*) 14 maggio (*conference call*) 18/20 giugno (Plenaria) 5 novembre(*conference call*) 27 ottobre (*ad hoc meeting*) 8/12 dicembre (Plenaria)
Consiglio d'Europa	Plenaria	2/4 giugno
	Comitato T-PD *Bureau*	25/27 marzo 30 settembre/1-2 ottobre 16/18 dicembre
	CAHDATA	28/30 aprile 1/3 dicembre
Gruppi di lavoro specifici	Gruppo internazionale di lavoro sulla protezione dei dati nelle telecomunicazioni (IWGDPT)	5 e 6 maggio 14 e 15 ottobre
	Privacy Risk Framework Project	20 marzo 18 novembre
International Enforcement	IECWG (*International Enforcement Coordination Working Group*)	16 gennaio (*conference call*) 17 marzo (*conference call*) 28 maggio (*conference call*) 13 giugno (*conference call*) 9 luglio (*conference call*) 20 agosto (*conference call*) 11 settembre (*conference call*)
	Progetto PHAEDRA	13 ottobre (*workshop*)
	GPEN (*Global Privacy Enforcement Network – Sweep*)	8 luglio (*conference call*) 20 agosto (*conference call*) 17 settembre (*conference call*) 3 dicembre (*conference call*)

Conferenze internazionali	
Conferenza di primavera delle Autorità europee di protezione dati	5 giugno, Strasburgo
35ª Conferenza internazionale delle Autorità di protezione dati	13/16 ottobre, Mauritius

Altre conferenze	
Case Handling Workshop	6 e 7 ottobre, Skopje
ICANN *Meeting*	12/16 ottobre, Los Angeles
European Data Governance Forum	8 dicembre, Parigi

€ 13,60