

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 aggiornare 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 aggiornare 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.

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.

OCSE

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 a 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.

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.

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.

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

Data retention – Expert Group

Cooperazione internazionale IECWG, GPEN, PHAEDRA project

GPEN

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 1º 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-

cià, 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*” (prov. 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/videojaranteprivacy), 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 YouTube 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.

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”.

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.

Forum PA

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*.

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

Anci

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:

- 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-

L'attività dell'Urp

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.