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