apposito decreto del Presidente del Consiglio dei Ministri, sul cui schema è stato consultato il Garante. Nel suo parere, l'Autorità ha sottolineato che il Sistema di allerta pubblico è volto a trasmettere, ai terminali presenti in una determinata area geografica, messaggi IT-*alert* riguardanti gli scenari di rischio, l'organizzazione dei servizi di protezione civile del proprio territorio e le misure di autoprotezione, escludendo l'utilizzo per finalità diverse da quelle ivi previste dei dati eventualmente raccolti. Tale trasmissione non comporta la conoscenza dei numeri di telefono dei terminali mobili contattati e, conseguentemente, nemmeno dell'identità dei contraenti o utenti delle reti di comunicazione mobile cellulare; pertanto, gli apparati di trasmissione di ciascun operatore potranno inviare il messaggio ai propri clienti, ma anche ai clienti di altri operatori di telefonia mobile, in modo del tutto indifferenziato, imprevedibile a priori e, comunque, non tracciabile. Il Sistema di allerta è basato, infatti, sul servizio di *cell broadcast*, disponibile sulle reti pubbliche di telefonia mobile perché previsto dall'architettura di rete GSM, come mezzo di distribuzione e consegna dei messaggi di allarme al dispositivo telefonico del destinatario, con l'invio di brevi messaggi di testo da parte di ciascuna "stazione base" (*Base Transceiver Station-BTS*) della rete pubblica. L'invio del messaggio di allerta avviene rispetto a tutti i dispositivi utente compresi in una determinata area geografica coperta dal segnale radio (cd. cella) in modalità *broadcast* e può essere ripetuto a intervalli di tempo prestabiliti per massimizzare la copertura dei dispositivi destinatari. Al fine di evitare fraintendimenti da parte degli utenti, la normativa tecnica stabilisce che i dispositivi riceventi devono essere in grado di cancellare i messaggi di allerta duplicati, ricevuti in un determinato intervallo di tempo.

Il Garante ha accolto con favore la misura prevista volta a consentire la disattivazione autonoma, da parte dell'interessato, della ricezione dei messaggi di allerta classificati di minore gravità, fermo restando che tale opzione di non visualizzazione di talune tipologie di messaggi *broadcast* debba essere garantita da impostazioni standard di trasmissione e settaggi dei dispositivi riceventi. È stato altresì rilevato che le misure tecniche e organizzative predisposte risultano idonee a garantire un livello di sicurezza adeguato ai rischi, con particolare riferimento alla necessaria certificazione dei messaggi che ne assevera la provenienza da fonti autorizzate.

Il Garante ha tuttavia ritenuto che, al fine di meglio garantire la correttezza e la trasparenza nei confronti dei destinatari dei messaggi, debba essere assicurata la più ampia conoscibilità delle informazioni relative alle modalità e alle finalità di invio dei messaggi attraverso il Sistema pubblico di allerta tramite specifiche campagne informative, chiarendo che la trasmissione *broadcast* dei messaggi non comporta la conoscenza dei numeri di telefono e dell'identità degli interessati, nonché evidenziando agli utenti le modalità di disattivazione dei messaggi di minore gravità (prov. 17 ottobre 2019, n. 193, doc. web n. 9207188).

4.4. Istruzione

Nel settore dell'istruzione il Garante ha interagito sia con il Miur che con università, istituzioni scolastiche ed altri soggetti pubblici nel corso di incontri e contatti volti a fornire chiarimenti e indicazioni in merito alla corretta applicazione della nuova disciplina in materia di protezione dei dati personali.

In tale ambito, particolare rilievo ha assunto il provvedimento 14 febbraio 2019, n. 44 (doc. web n. 9102421) con il quale il Garante ha espresso, ai sensi dell'art. 36, par. 4, del RGPD, parere favorevole su uno schema di regolamento predisposto

4

Invalsi

4

dall'Istituto nazionale per la valutazione del sistema educativo di istruzione e di formazione, concernente le modalità di svolgimento delle prove Invalsi dell'ultimo anno della scuola secondaria di secondo grado (cd. grado 13). Lo schema di regolamento presentato ha riprodotto i meccanismi previsti nel regolamento della prova Invalsi del terzo anno della scuola secondaria di primo grado (cd. grado 8) del 16 febbraio 2018, in merito al quale il Garante si era espresso con parere favorevole 15 febbraio 2018, n. 76 (doc. web n. 8081291), differenziandosi da quest'ultimo solo in relazione alla classe in cui le prove vengono somministrate (quinto anno della scuola secondaria di secondo grado). Sono così dettate le regole relative allo svolgimento delle prove Invalsi della "quinta superiore" e si disciplinano, in particolare: le modalità di identificazione dello studente ai fini del corretto espletamento e della restituzione delle prove che, nel caso di alunni con disabilità e di alunni con disturbi specifici di apprendimento (Dsa), possono essere personalizzate; lo svolgimento delle prove, prevedendo che l'Invalsi predisponga un documento contenente informazioni che consentono la sicura identificazione di ciascuno studente; le modalità e i tempi di conservazione dei dati da parte di Invalsi, prevedendo la cancellazione del nome e del cognome degli studenti una volta terminato lo svolgimento delle prove; il trattamento di categorie particolari di dati personali, specificando che il trattamento dei dati relativi alla salute è effettuato in attuazione dello schema di regolamento da parte dell'Invalsi e delle scuole, in qualità di autonomi titolari del trattamento per gli aspetti di competenza, per i motivi di interesse pubblico rilevante di cui all'art. 2-*sexies* del Codice.

Diffusione di dati personali

L'Ufficio ha ricevuto, inoltre, numerosi reclami e segnalazioni aventi a oggetto la diffusione, sul sito web istituzionale di taluni istituti scolastici, di graduatorie d'istituto relative al personale docente o al personale amministrativo, tecnico e ausiliario (Ata), contenenti anche informazioni relative all'indirizzo di residenza, al numero di telefono fisso o di cellulare, all'indirizzo *e-mail* del personale nonché (a seguito degli approfondimenti effettuati) all'indicazione dei titoli di preferenza del personale scolastico e ai dati relativi alla salute dei docenti, contrariamente a quanto previsto dal Codice che ne vieta esplicitamente la diffusione. In seguito all'intervento dell'Autorità, gli istituti scolastici hanno prontamente rimosso tali dati dal sito istituzionale. Graduatorie di docenti e dati personali relativi a docenti sono stati diffusi anche da taluni uffici scolastici regionali.

In tutte le ipotesi richiamate, facendo seguito agli approfondimenti effettuati, l'Ufficio ha proceduto alla notifica di violazione ai sensi dell'art. 166 del Codice con conseguente avvio del procedimento per l'adozione di provvedimenti correttivi/sanzionatori. La diffusione di dati personali è stata inoltre oggetto di verifiche, effettuate dal Garante e culminate con la notifica della violazione ai sensi del richiamato art. 166 del Codice, in relazione a reclami riguardanti ipotesi di diffusione di dati personali, anche relativi alla salute, riguardanti studenti, nonché la diffusione di informazioni concernenti le valutazioni intermedie di candidati a una procedura selettiva bandita da un'università.

Esercizio dei diritti

Numerose le richieste di intervento in relazione al mancato riscontro, da parte del titolare del trattamento, a richieste di esercizio dei diritti in materia di protezione dei dati personali, ai sensi degli artt. 15-22 del RGPD. A seguito delle verifiche istruttorie, gli interessati sono stati invitati a esercitare i diritti con istanza rivolta al titolare e, in altri casi, è stato rivolto al titolare del trattamento l'invito ad aderire spontaneamente alla richiesta formulata dall'interessato. Quando la mancata risposta o il ritardo nel riscontro all'interessato è apparso non giustificato, si è proceduto all'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del RGPD.

4

Uno dei casi di esercizio dei diritti ha riguardato l'istanza di accesso all'elaborato scritto dell'istante relativo alla prova di italiano sostenuta durante l'esame di maturità. Nella trattazione del caso l'Ufficio ha tenuto conto dell'orientamento della Corte di Giustizia dell'Unione europea (cfr. CGUE 20 dicembre 2017, C-434/16) che, chiamata in via pregiudiziale ad esprimersi in merito alla natura di "dati personali" ai sensi della direttiva 95/46 delle informazioni contenute nelle risposte fornite da un candidato durante un esame, si è espressa affermativamente attribuendo alla locuzione un'accezione estesa, tale da comprendere "potenzialmente ogni tipo di informazioni, tanto oggettive che soggettive, sotto forma di pareri o di valutazioni, a condizione che esse siano concernenti la persona interessata" e che "le risposte scritte fornite da un candidato nel corso di un esame professionale e le eventuali annotazioni dell'esaminatore relative a tali risposte costituiscono dati personali. Secondo la Corte, il contenuto di tali risposte riflette, infatti, "il livello di conoscenza e di competenza del candidato in un dato settore nonché, se del caso, i suoi processi di riflessione, il suo giudizio e il suo spirito critico. In caso di esame redatto a mano le risposte contengono, inoltre informazioni morfologiche". La Corte ha inoltre affermato che: "va constatato, poi, che i diritti di accesso e di rettifica [...] possono anch'essi trovare giustificazione per quanto riguarda le risposte scritte fornite da un candidato durante un esame professionale [...]". In precedenza anche l'Autorità si era espressa sul punto con il parere 26 ottobre 2017, n. 433 (doc. web n. 7156158) affermando che per gli specifici profili inerenti l'accesso civico alla copia degli elaborati scritti del concorso pubblico, si deve tenere altresì presente che in generale l'elaborato scritto presentato a un concorso pubblico è, in linea di massima, indicativo anche di molteplici aspetti di carattere personale circa le caratteristiche individuali, relativi ad esempio alla preparazione professionale, alla cultura, alle capacità di espressione, o al carattere del candidato, che costituiscono aspetti valutabili nella selezione dei partecipanti. Inoltre, in alcuni casi, e a seconda della traccia sottoposta, il contenuto degli elaborati può essere potenzialmente capace di rivelare anche informazioni e convinzioni che possono rientrare nella categoria dei dati sensibili di cui all'art. 4, comma 1, lett. d), del Codice (si pensi alle tracce su temi storici o di cultura generale che potrebbero rivelare "opinioni politiche" o "convinzioni filosofiche o di altro genere").

4.5. *La trasparenza amministrativa e la pubblicità dell'azione amministrativa*

Numerose continuano ad essere le questioni esaminate riguardanti il tema della protezione dei dati personali con riferimento alle esigenze di trasparenza e di pubblicità dell'azione amministrativa che, per esigenze di chiarezza espositiva, si esamineranno distinguendo, da un lato, la materia della pubblicazione di dati personali *online* e, dall'altro, l'accesso a informazioni e documenti detenuti dalla p.a. tramite gli strumenti dell'accesso civico (art. 5, d.lgs. 14 marzo 2013, n. 33) nonché dell'accesso ai documenti amministrativi (artt. 22 ss., l. 7 agosto 1990, n. 241), dandosi qui conto solo dei casi più rilevanti conclusi con provvedimento del Collegio.

4.5.1. *La pubblicazione di dati personali online*

Tra i casi rispetto ai quali l'Autorità è stata chiamata a pronunciarsi, si è nuovamente presentata la questione della diffusione *online* di dati personali da parte di soggetti pubblici in assenza di un idoneo presupposto normativo (norma di legge o di regolamento). Il Garante ha in proposito censurato il comportamento di un comune che aveva pubblicato sull'albo pretorio *online* una deliberazione

4

della giunta comunale, contenente dati personali non necessari, quali l'esistenza di un procedimento penale (peraltro archiviato) a carico del segnalante dipendente comunale la cui pubblicazione si è protratta per un periodo di tempo superiore ai quindici giorni previsti dalla normativa di settore (art. 124, d.lgs. 18 agosto 2000, n. 267). È stato rilevato che tale condotta configurava una violazione dei principi di liceità e minimizzazione del trattamento (art. 5, par. 1, lett. *a* e *c*), del RGPD) nonché dell'art. 6, par. 1, lett. *c*) ed *e*); par. 2 e par. 3, lett. *b*), del RGPD, considerando che erano stati diffusi dati personali in assenza di un idoneo presupposto normativo (per il periodo eccedente i tempi di pubblicazione previsti dall'art. 124, comma 1, d.lgs. n. 267/2000) in violazione dell'art. 19, comma 3, del Codice (vigente all'epoca dei fatti, ma il cui contenuto è confluito con analoghe disposizioni nell'art. 2-ter, commi 1 e 3, del Codice). In relazione ai predetti elementi, ai sensi dell'art. 83, del RGPD, è stata comminata all'ente locale la sanzione amministrativa di 6.000,00 euro (con possibilità di definire la controversia mediante il pagamento di un importo pari alla metà della sanzione irrogata ai sensi dell'art. 166, comma 8, del Codice): ciò in quanto la gravità del comportamento tenuto non poteva essere bilanciata dalle giustificazioni fornite dall'amministrazione titolare del trattamento (secondo cui la violazione sarebbe stata causata da un errore di valutazione da parte del responsabile del procedimento e da un errore informatico commesso dalla società incaricata della pubblicazione); per la determinazione dell'importo della sanzione, alla luce di quanto previsto dall'art. 83, par. 2, del RGPD, sono state tenute in considerazione ulteriori circostanze, fra cui il carattere non doloso dell'illecita diffusione che, pur protrandosi per oltre un anno, aveva tuttavia riguardato un solo interessato. Inoltre sono state valutate positivamente l'immediata rimozione dei dati dal sito web, la collaborazione offerta dal titolare del trattamento nel corso dell'istruttoria, l'adozione di diverse misure tecniche e organizzative messe in atto ai sensi degli artt. 25-32, del RGPD nonché l'assenza di precedenti violazioni (prov. 7 novembre 2019, n. 209, doc. web n. 9269824).

4.5.2. L'accesso civico

In materia di diritto di accesso civico e protezione dei dati personali il Garante è intervenuto in occasione dell'approvazione di numerosi pareri resi ai Responsabili della prevenzione della corruzione e della trasparenza (Rpct) o a Difensori civici ai sensi dell'art. 5, commi 7 e 8, d.lgs. n. 33/2013.

Come in passato, il Garante ha invitato l'amministrazione a rivalutare dinieghi a richieste di accesso civico che, pur basati sulla protezione dei dati personali, non erano però adeguatamente motivati (cfr., fra i tanti, parere 13 agosto 2019, n. 160, doc. web n. 9157176).

L'Autorità ha poi ribadito che il limite all'accesso civico derivante dalla protezione dei dati personali non trova applicazione a soggetti diversi dalle persone fisiche. Su tale assunto un'amministrazione è stata invitata a rivalutare il proprio provvedimento di diniego parziale su un'istanza di accesso civico generalizzato volta a ottenere un verbale di violazione amministrativa elevato nei confronti di un circo per l'affissione di cartelli pubblicitari (parere 29 maggio 2019, n. 122, doc. web n. 9128783; sulle persone giuridiche cfr. anche parere 21 febbraio 2019, n. 47, doc. web n. 9103063).

Fra i casi in cui è stata ritenuta non provata l'esistenza di un pregiudizio concreto alla protezione dei dati personali va annoverato il parere reso su una richiesta di accesso civico avente a oggetto la copia dei provvedimenti adottati nei confronti di alcuni amministratori locali per ottenere il recupero delle somme da restituire in virtù della rideterminazione di indennità di carica nonché dei pagamenti effettuati

Persone giuridiche

Politici

ai fini della restituzione delle somme dovute. In questo caso la p.a. è stata invitata a rivalutare il diniego opposto, previo coinvolgimento dei soggetti controinteressati, fornendo una motivazione congrua e completa rispetto all'esistenza o meno del limite di cui all'art. 5-bis, comma 2, lett. a), d.lgs. n. 33/2013. Ciò tenendo conto, quali elementi favorevoli all'ostensione, della circostanza che alcune informazioni erano già oggetto di pubblicazione obbligatoria; del ruolo, della funzione pubblica e dell'attività di pubblico interesse esercitata dagli amministratori locali cui si riferivano i dati personali oggetto di accesso; del regime di pubblicità e trasparenza rafforzato richiesto per coloro che rivestono incarichi di indirizzo politico in relazione ai compensi percepiti. È stato inoltre evidenziato che, per effettuare la valutazione, è necessario in ogni caso rispettare il principio di minimizzazione, alla luce del quale i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità di trasparenza propria dell'istituto dell'accesso civico, in modo che non si realizzi un'interferenza ingiustificata e sproporzionata nei diritti e nelle libertà delle persone, tenendo altresì conto dell'eventuale esistenza di contenziosi ancora in corso attivati dai controinteressati in merito alla richiesta di restituzione di parte delle indennità percepite e dell'interferenza che la conoscibilità di questi dati poteva determinare sul diritto di difesa (parere 26 giugno 2019, n. 145, doc. web n. 9126414).

Analogamente, anche se in relazione a una fattispecie diversa, a fronte del diniego di una richiesta di accesso civico avente a oggetto diversi documenti di un'agenzia regionale, inerenti alla determinazione di indizione e al bando di concorso per le progressioni economiche orizzontali del personale nonché all'atto di nomina della commissione esaminatrice delle candidature, non si è ravvisato con riferimento all'atto di nomina della commissione, il rischio del pregiudizio concreto alla tutela dei dati personali; mentre nel caso del bando, trattandosi di documento non contenente dati personali, non poteva in alcun caso essere richiamato il limite all'accesso civico di cui all'art. 5-bis, comma 2, lett. a), d.lgs. n. 33/2013 (parere 28 febbraio 2019, n. 48, doc. web n. 9103079).

In relazione, inoltre, a una istanza di riesame proposta a seguito di un diniego su una istanza di accesso civico generalizzato volta conoscere gli anni accademici in cui un soggetto aveva tenuto alcune docenze presso un'università, è stato rappresentato che dalla motivazione fornita dall'amministrazione non si desumeva il motivo per cui l'ostensione dell'informazione richiesta potesse recare un pregiudizio concreto alla protezione dei dati personali del controinteressato. Ciò considerando che l'informazione relativa alla docenza (compresa la materia oggetto di insegnamento) era già liberamente accessibile nelle note bibliografiche riferite al soggetto controinteressato presenti su diversi siti di informazione *online* (parere 14 novembre 2019, n. 205, doc. web n. 9207868).

Numerosi i casi in cui è stato confermato il diniego totale o parziale di richieste di accesso civico alla luce dei limiti derivanti dalla normativa in materia di protezione dei dati personali; anche rispetto ad essi si darà di seguito conto solo dei casi più significativi, dividendoli per aree tematiche.

Per l'estrema delicatezza della questione, merita ricordare il parere reso in relazione a una istanza di accesso civico volta a ottenere dati e informazioni personali di bambini di nazionalità estera giunti in Italia con un convoglio umanitario e dati in affido educativo in specifici centri per essere successivamente adottati. Al riguardo, è stato evidenziato che la normativa di settore prevede un divieto di comunicazione di informazioni relative ai bambini adottati, laddove sancisce che l'ufficiale di stato civile e l'ufficiale di anagrafe nonché "qualsiasi altro ente pubblico o privato, autorità o pubblico ufficio" devono "rifiutarsi di fornire notizie, informazioni, cer-

4

Commissioni di concorso

Contratti di docenza

Persone adottate o in affidamento educativo

4

**Atti di una commissione
etica di un ateneo**

tificazioni, estratti o copie dai quali possa comunque risultare il rapporto di adozione, salvo autorizzazione espressa dell'Autorità giudiziaria" (art. 28, comma 3, l. n. 184/1983). Pertanto, tale fattispecie rientrava in una delle ipotesi di cui all'art. 5-bis, comma 3, d.lgs. n. 33/2013, che prevede l'esclusione dell'accesso nei "casi di divieti di accesso o divulgazione previsti dalla legge". In relazione invece alle altre informazioni riguardanti bambini interessati dalla vicenda ma non afferenti all'adozione, è stato osservato che in ogni caso si trattava di dati personali delicati, riferiti a soggetti vulnerabili, la cui ostensione, anche parziale, poteva arrecare agli stessi – seppure oggi maggiorenni – ripercussioni negative sul piano sociale, relazionale e professionale, in considerazione del particolare regime di pubblicità dei dati oggetto di accesso civico nonché delle ragionevoli aspettative di confidenzialità dei soggetti interessati (parere 7 febbraio 2019, n. 26, doc. web n. 9100178).

Analogamente, per la particolarità della fattispecie, si segnala l'intervento del Garante su due richieste di accesso civico riguardanti la documentazione della commissione etica di un ateneo, relativa a una procedura volta a verificare il rispetto del codice etico da parte di un soggetto. Richiamando i precedenti pareri in materia di sanzioni disciplinari (v. provv.ti 21 novembre 2018, n. 483; 7 dicembre 2017, n. 515; 31 maggio 2017, n. 254), è stato affermato che la generale conoscenza delle informazioni richieste violava il dovere di riservatezza della commissione e determinava un'interferenza sproporzionata nei diritti e nelle libertà dei controinteressati. Ciò tenendo in considerazione le ragionevoli aspettative di confidenzialità dell'interessato (che si era peraltro rivolto spontaneamente alla commissione) e degli altri soggetti coinvolti nella vicenda, i quali potevano fare ragionevolmente affidamento sul carattere riservato del procedimento. Nel caso di specie, il principio di trasparenza è apparso soddisfatto dalla conoscenza dell'esito del procedimento, avviato e concluso, che l'università aveva provveduto ad assicurare. L'ulteriore documentazione di cui si richiedeva l'ostensione, invece, contenendo dati e informazioni personali delicate, poteva effettivamente arrecare un pregiudizio concreto alla tutela della protezione dei dati personali, anche in ragione del particolare regime di pubblicità dei dati oggetto di accesso civico. La probabilità di tale pregiudizio, inoltre, era amplificata dalla notorietà a livello locale che la vicenda aveva assunto su una testata giornalistica *online* e dalla circostanza di poter causare danni legati alla sfera morale, relazionale, professionale e sociale dell'interessato e delle altre persone coinvolte sia all'interno che all'esterno della comunità scientifica di appartenenza. Tali considerazioni impedivano altresì di accordare un accesso civico parziale, oscurando i nominativi dei controinteressati, in quanto questi ultimi risultavano comunque indirettamente identificabili, anche all'interno del luogo di lavoro, attraverso gli ulteriori dati di contesto o le informazioni di dettaglio contenute nei documenti richiesti (pareri 10 ottobre 2019, n. 184, doc. web n. 9195259 e 31 ottobre 2019, n. 196, doc. web n. 9195266).

**Denunce all'Autorità
giudiziaria**

Altra fattispecie di interesse riguarda l'accesso civico alle denunce presentate da un comune, nel caso di specie anche contro ignoti, all'Autorità giudiziaria (o ad un'altra autorità competente), negli anni 2017-2019, per reati ambientali avvenuti nel territorio dell'ente. L'amministrazione aveva negato l'ostensione, rappresentando che gli atti richiesti erano stati trasmessi al Comando dei Carabinieri per la tutela dell'ambiente con riferimento a un'indagine della Procura della Repubblica. Pertanto le informazioni richieste potevano essere coperte da segreto istruttorio. Il soggetto istante è stato quindi invitato a rivolgere al tribunale eventuali richieste di accesso nei termini e modi previsti dalla legge. Il Garante, pur non entrando nel merito del diniego opposto, ha evidenziato che, in ogni caso, i documenti di cui si chiedeva l'accesso civico potevano contenere dati e informazioni personali di tutti

coloro che erano stati destinatari delle predette denunce (tranne per le denunce contro ignoti). Si poteva trattare quindi di documenti – contenenti dati e informazioni delicate – riferiti a soggetti nei cui confronti poteva essere aperto un procedimento penale e la cui generale conoscenza poteva, di conseguenza, causare un pregiudizio alla tutela dei dati personali, quali danni legati alla sfera morale, relazionale, professionale e sociale, gettando discredito sui controinteressati anche nel caso di denunce poi archiviate. Il Garante ha invece ritenuto non sussistere alcuna ragione attinente alla protezione dei dati personali in relazione all'eventuale ostensione di dati aggregati (privi di dati identificativi e di ogni ulteriore informazione idonea a identificare i controinteressati anche indirettamente), quali ad esempio il numero delle denunce effettuate negli ultimi tre anni e la relativa data (parere 10 ottobre 2019, n. 187, doc. web n. 9198109).

Tra i pareri più significativi c'è, inoltre, quello in materia di accesso civico presentato a un'azienda sanitaria avente ad oggetto dati relativi alla salute (quadro clinico, dettagli su ricovero, degenza, sintomi, anamnesi, diagnosi, esami effettuati, terapia, farmaci somministrati, consulenze mediche effettuate, ecc.) di un paziente, poi deceduto. In particolare, è stato affermato che il riconoscimento della possibilità di esercitare i diritti in materia di protezione dei dati personali (artt. 15-22, del RGPD) da parte dei soggetti elencati nell'art. 2-terdecies, comma 1, del Codice, comporta – quale naturale conseguenza e necessario presupposto logico-giuridico – che ai dati personali concernenti le persone decedute continuino ad applicarsi le tutele previste dalla disciplina in materia di protezione dei dati personali. Per tale motivo, considerando che l'art. 2-septies, comma 8, del Codice prevede un divieto di diffusione di dati idonei a rivelare lo stato di salute, è stato confermato il diniego dell'azienda all'accesso civico generalizzato ai predetti dati personali ancorché riferiti a un paziente poi deceduto, in forza del richiamo operato dall'art. 5-bis, comma 3, d.lgs. n. 33/2013, secondo il quale l'accesso va escluso, fra l'altro, nei casi di divieto di divulgazione espressamente previsti da normative di settore (parere 10 gennaio 2019, n. 2, doc. web n. 9084520; in materia di dati sulla salute, cfr. anche parere 7 febbraio 2019, n. 27, doc. web n. 9090308, in cui è evidenziata la diversa tipologia di valutazione che l'amministrazione deve invece effettuare quando l'accesso è richiesto ai sensi della diversa legge n. 241/1990).

Cambiando materia, molto frequenti sono state le richieste di parere in ordine all'accesso civico a dati e informazioni personali riferite a dipendenti, lavoratori e soggetti che hanno avuto contratti o rapporti con la p.a. Al riguardo, è stata più volte affermata la sussistenza di un pregiudizio concreto alla protezione dei dati personali, in considerazione della tipologia e della natura dei dati e delle informazioni personali oggetto dell'istanza, del particolare regime di pubblicità che connota l'accesso civico nonché delle ragionevoli aspettative di confidenzialità dei soggetti controinteressati sui quali si potevano realizzare ripercussioni negative sul piano sociale, relazionale o professionale. È stata altresì evidenziata la necessità di rispettare il principio di minimizzazione dei dati, in base al quale i dati devono essere, fra l'altro, "limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. c), del RGPD) e l'impossibilità di accordare un accesso parziale, oscurando i nominativi dei controinteressati, in quanto questi sarebbero risultati indirettamente identificabili, anche all'interno del luogo di lavoro, attraverso gli ulteriori dati di contesto o informazioni di dettaglio contenute nei documenti richiesti. In molti casi, l'amministrazione è stata invitata a fornire, comunque, dati aggregati (privi di dati e informazioni tali da identificare i soggetti interessati anche indirettamente), al fine di dare soddisfazione all'interesse conoscitivo del soggetto istante. In generale, è stato più volte rappresentato che in presenza di un interesse specifico del

4

Soggetti deceduti

Rapporto di lavoro

4

Dati di dipendenti e
altre ipotesi

soggetto istante, laddove i documenti non possano essere forniti mediante l'istituto dell'accesso civico generalizzato, resta in ogni caso salva la possibilità di accedere alla documentazione richiesta ai sensi della disciplina in materia di accesso agli atti amministrativi contenuta negli artt. 22 ss., l. n. 241/1990 dimostrando l'esistenza di "un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso".

Il Garante ha condiviso il diniego opposto da un comune all'accesso civico avente a oggetto una comunicazione fornita all'ente da un proprio dipendente contenente dati personali allo stesso riferiti nonché ulteriori informazioni relative anche alla capacità professionale, alle prospettive di carriera e a iniziative svolte all'esterno dell'amministrazione di appartenenza (parere 7 febbraio 2019, n. 29, doc. web n. 9086520). Analogamente è stato ritenuto sussistente un pregiudizio alla protezione dei dati personali dei controinteressati, in ragione del quale l'amministrazione ha correttamente rifiutato l'accesso civico generalizzato, in relazione a istanze aventi ad oggetto, fra l'altro:

- il nulla osta e il parere tecnico relativo alla mobilità di un dipendente (parere 19 marzo 2019, n. 63, doc. web n. 9114118);
- i fogli presenza dei dipendenti, i giorni e le ore di lavoro oppure le mansioni svolte (pareri 14 marzo 2019, n. 60, doc. web n. 9102014; 10 ottobre 2019, n. 185, doc. web n. 9198091);
- le date di assunzione e cessazione dell'incarico di un dipendente ministeriale (parere 10 ottobre 2019, n. 186, doc. web n. 9198098);
- l'ostensione di tutte le contestazioni disciplinari e dei provvedimenti a esse conseguenti emesse, nei cinque anni anteriori alla richiesta, da un'azienda partecipata da un comune (parere 16 agosto 2019, n. 161, doc. web n. 9161714);
- l'elenco nominativo (o il numero di matricola con ruolo professionale) dei dirigenti di un'azienda presi a riferimento per la costituzione di quattro fondi di risultato delle distinte aree, il numero di ore di plus orario assegnate individualmente nonché il valore economico di ciascuna ora (parere 12 settembre 2019, n. 164, doc. web n. 9157101);
- i documenti di carattere prodromico e funzionale all'approvazione di graduatoria per la progressione economica orizzontale del personale amministrativo dipendente di un'agenzia regionale (parere 28 febbraio 2019, n. 48, doc. web n. 9103079);
- i documenti inerenti alla liquidazione della produttività strategica di un ex dipendente e alla liquidazione di incarichi a professionisti risalenti nel tempo, come indicato nei pareri 7 marzo 2019, n. 54 (doc. web n. 9102429) e 7 febbraio 2019, n. 28 (doc. web n. 9086500); nel secondo caso il pregiudizio era aggravato dall'esistenza di vicende giudiziarie intercorrenti fra il soggetto istante e il soggetto controinteressato;
- i dati "relativi alla spendita delle procure e alla partecipazione alle udienze nei tre gradi di giudizio, per il 2017 e 2018" di tutti gli avvocati che hanno ricevuto la procura alle liti dell'Inps, anche considerando che le informazioni richieste potevano far conoscere la distribuzione dei carichi di lavoro fra i singoli legali, con conseguente possibilità di individuare il trattamento economico dagli stessi percepito nonché, in alcuni casi, anche le situazioni personali rappresentate, ad esempio, da periodi di assenza dal servizio per malattia (parere 19 marzo 2019, n. 62, doc. web n. 9115506);
- i documenti inerenti alla partecipazione a una procedura di gara per l'affidamento di un contratto pubblico contenente dati, informazioni e documenti di diversa specie, riferiti a più di 1.700 persone, riguardanti, in particolare, la

lista del personale utilizzato nei vari servizi, il *curriculum vitae* del personale, la documentazione comprovante il possesso dei titoli, competenze ed esperienze previste per le varie figure professionali, la documentazione richiesta per il personale addetto a specifici servizi (parere 23 maggio 2019, n. 115, doc. web n. 9124946);

- gli atti relativi a un concorso di dottorato di ricerca, quali copia degli elaborati delle prove scritte, dei verbali di correzione degli elaborati e dei *curricula vitae* dei candidati (parere 7 novembre 2019, n. 200, doc. web n. 9196072).

Si menzionano, infine, i numerosi pareri resi su istanze di accesso civico aventi ad oggetto interventi urbanistici, titoli e abusi edilizi, nonché concessioni demaniali. Nel corso del 2019 il Garante è in più occasioni tornato a occuparsi del tema dell'accesso civico generalizzato alla documentazione inerente a Segnalazioni certificate di inizio attività (Scia) e a Certificazioni di inizio attività asseverata (Cila), evidenziando che i casi in cui è necessario presentare l'una o l'altra interessano un insieme molto variegato di interventi edilizi, spaziando dalla semplice apertura o chiusura di un vano finestra, alla costruzione di una recinzione, al frazionamento o accorpamento di unità abitative, fino a operazioni più importanti come il rifacimento di tetti o solai, oppure la ristrutturazione generale di un intero fabbricato. Pertanto, le informazioni e i dati, anche di carattere personale, da presentare all'ente competente, e contenuti nei predetti titoli abilitativi edilizi (Cila e Scia), sono molteplici e di diverso genere e natura, quali, ad esempio, nominativi, data e luogo di nascita, codici fiscali, residenza, *e-mail*, Pec, numeri di telefono fisso e cellulare riferiti al/i titolare/i dell'intervento in qualità di proprietario, comproprietario, usufruttuario, amministratore di condominio o dei loro rappresentanti; informazioni sulla tipologia di intervento; data di inizio e fine dello stesso; ubicazione, dati catastali e destinazione d'uso dell'immobile oggetto dell'intervento edilizio; carattere oneroso o gratuito dell'intervento, eventuale ricezione dei versamenti effettuati; entità presunta del cantiere; dati dei tecnici incaricati (direttori dei lavori e altri tecnici) e dell'impresa esecutrice dei lavori; prospetto di calcolo preventivo del contributo di costruzione e elaborati grafici dello stato di fatto e progetto.

In merito, è stato ribadito che non esiste un obbligo di pubblicazione da parte delle pp.aa. delle Scia o delle Cila presentate all'ente (né in forma integrale, né in forma riassuntiva) e che per i dati personali ivi contenuti il legislatore non ha previsto alcun regime di pubblicità. Ciò in quanto la disposizione contenuta nell'art. 20, comma 6, d.P.R. n. 380/2001 (Testo unico in materia edilizia) è una norma di settore attinente al solo "procedimento per il rilascio del permesso di costruire", che costituisce un titolo edilizio diverso dalla Cila e dalla Scia. Inoltre, la predetta disposizione, che non è ripetuta (né richiamata) per i procedimenti relativi agli altri titoli edilizi (Cila o Scia), non prevede neanche la pubblicazione del provvedimento sull'albo pretorio nella sua integrità, ma della mera "notizia" dell'"avvenuto rilascio del permesso di costruire" (i cui estremi sono peraltro "indicati nel cartello esposto presso il cantiere, secondo le modalità stabilite dal regolamento edilizio"). Alla Cila e alla Scia – disciplinate nel medesimo d.P.R. n. 380/2001 – non è di conseguenza in nessun modo applicabile il limitato regime di pubblicità previsto per la "notizia" dell'avvenuto rilascio del permesso di costruire.

Con riferimento ai casi esaminati, è stato nuovamente affermato che non è possibile accordare una generale prevalenza della trasparenza o del diritto di accesso civico generalizzato a scapito di altri diritti ugualmente riconosciuti dall'ordinamento, in quanto si vanificherebbe il necessario bilanciamento degli interessi che richiede un approccio equilibrato nella ponderazione dei diversi diritti coinvolti. In tale quadro, rispetto all'esistenza del limite dalla tutela dei dati personali a fronte del

4

Scia e Cila

4

quale dover rifiutare un accesso civico generalizzato, è stato ricordato che devono essere tenuti in considerazione: la circostanza che i dati e le informazioni fornite all'esito dell'accesso civico generalizzato sono pubblici e tendenzialmente riutilizzabili; il rispetto del principio di minimizzazione dei dati personali; le ragionevoli aspettative di confidenzialità dei controinteressati in relazione al trattamento dei propri dati personali al momento in cui questi sono stati raccolti; la non prevedibilità delle conseguenze derivanti dall'eventuale conoscibilità da parte di chiunque dei dati richiesti. Ciò anche in ragione del fatto che, nel caso esaminato, il richiedente era un'impresa che svolgeva attività di gestione di *database* e di *marketing* e che risultava aver effettuato, con carattere sistematico, analoghe richieste a tutte le Scia e alle Cila di diversi enti locali. Tale circostanza poteva causare un pericolo di duplicazione di banche dati di soggetti pubblici da parte di soggetti privati in assenza del consenso degli interessati o degli altri presupposti di liceità del trattamento previsti dall'art. 6, par. 1, del RGPD, nonché il possibile rischio di "usi impropri" e/o di "riutilizzo" e trattamento ulteriore dei dati personali per finalità non compatibili con quelle per le quali i dati personali erano stati inizialmente raccolti e in contrasto con quanto previsto dall'art. 6, par. 4, del RGPD. Il Garante ha quindi condiviso la scelta dell'amministrazione di respingere l'istanza di accesso civico in quanto l'ostensione dei dati richiesti poteva effettivamente arrecare ai controinteressati quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-bis, comma 2, lett. a), d.lgs. n. 33/2013. Come già osservato in passato, è stato ribadito che le informazioni di dettaglio contenute nelle Scia e nelle Cila impediscono di poter accordare un eventuale accesso civico ai sensi dell'art. 5-bis, comma 4, d.lgs. n. 33/2013, anche oscurando, ad esempio, i dati identificativi (nome e cognome) del committente o del tecnico progettista. Tale accorgimento, infatti, non elimina la possibilità che i soggetti interessati siano identificati indirettamente tramite gli ulteriori dati di contesto contenuti nella documentazione richiesta. È apparso invece conforme alla normativa in materia di protezione dei dati personali la soluzione adottata dall'amministrazione comunale che – allo scopo di soddisfare comunque le esigenze informative alla base dell'accesso civico e di "favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico" (art. 5, comma 2, d.lgs. n. 33/2013) – ha fornito i dati relativi alle Scia e Cila, senza comunicare dati personali, e precisamente: la tipologia di titolo edilizio (Scia o Cila), una descrizione dell'intervento (es: manutenzione straordinaria, installazione insegna; intervento miglioramento sismico, nuovo accesso carraio, variante in corso d'opera per ristrutturazione edilizia; opere interne; variante in corso d'opera, ecc.), le informazioni relative all'effettuazione dell'intervento nel comune o in una sua frazione (parere 3 gennaio 2019, n. 1, doc. web n. 9080951; cfr. anche parere 12 settembre 2019, n. 162, doc. web n. 9157164; parere 24 gennaio 2019, n. 12, doc. web n. 9084347).

Abusi edilizi

Sempre in tema di edilizia, il Garante è stato chiamato a intervenire in relazione a una richiesta di accesso civico generalizzato ai verbali di abusi edilizi e ai relativi provvedimenti adottati negli anni 2018 e 2019; anche in tale fattispecie è stato condiviso il diniego opposto da un comune, in quanto l'ostensione dei dati personali contenuti nella documentazione, unita al particolare regime di pubblicità dei dati oggetto della richiesta, poteva causare, a seconda delle ipotesi e del contesto in cui i dati e le informazioni possono essere utilizzate, un pregiudizio concreto alla tutela della protezione dei dati personali. Non sussistevano invece ragioni attinenti alla protezione dei dati personali in relazione all'ostensione di dati aggregati, quali ad esempio il numero degli abusi edilizi rilevati negli ultimi due anni e le aree/zone

comunali interessate prive di indirizzi e numeri civici (parere 18 dicembre 2019, n. 220, doc. web n. 9232553).

Merita segnalare infine il parere in materia di concessioni demaniali nel quale il Garante ha ritenuto corretto il diniego di un'istanza di accesso civico generalizzato tesa a ottenere copia degli atti delle concessioni demaniali marittime di stabilimenti e chioschi, comprese le relative planimetrie dagli anni 2000, nonché tutte le concessioni per atto formale complete di allegati, rilasciate da un comune. Ciò in quanto l'accesso civico generalizzato ai dati personali contenuti nella documentazione richiesta, unito alla generale conoscenza e al particolare regime di pubblicità dei dati oggetto di accesso civico, poteva costituire un'interferenza sproporzionata nei diritti e libertà dei controinteressati, arrecando a questi ultimi, a seconda delle ipotesi e del contesto di utilizzazione delle informazioni fornite da parte di terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall'art. 5-*bis*, comma 2, lett. *a*), d.lgs. n. 33/2013 (parere 2 ottobre 2019, n. 179, doc. web n. 9162546).

4.5.3. L'accesso ai documenti amministrativi

Quanto al diverso accesso ai documenti amministrativi ai sensi degli artt. 22 ss., l. n. 241/1990, continuano a pervenire al Garante richieste di parere da parte di amministrazioni o di singoli cittadini rispetto alle quali, come in passato, è stato evidenziato che le norme in materia di accesso ai documenti amministrativi non sono state modificate dal nuovo quadro normativo in materia di protezione dei dati personali (artt. 22 ss., l. n. 241/1990; d.P.R. 12 aprile 2006, n. 184; artt. 6, 9, 10 e 86 del RGPD; artt. 59 e 60 del Codice). In particolare, l'art. 86 del RGPD prevede che "i dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico [...] per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità [...] conformemente al diritto dell'Unione o degli Stati membri [...] al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione di dati personali". Inoltre, l'art. 59, comma 1, del Codice precisa che "fatto salvo quanto previsto dall'art. 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241 [...] anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del Regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso".

È stato pertanto ribadito che spetta all'amministrazione, e non al Garante, nel caso di richieste di accesso ai documenti presentate ai sensi della legge n. 241/1990, accertare l'esistenza nel caso concreto dell'interesse qualificato, alla luce dei motivi sottesi alla richiesta, nonché verificare la sussistenza di una delle ragioni per le quali il documento richiesto può essere sottratto alla conoscibilità del richiedente, anche in base alle tipologie di documenti non accessibili individuati nell'apposito regolamento della singola amministrazione. È stato inoltre precisato che le valutazioni in ordine alle determinazioni adottate dalle amministrazioni sulle specifiche richieste di accesso esulano dall'ambito di competenza del Garante e rimangono sindacabili di fronte alle autorità competenti (art. 25, l. n. 241/1990).

4.6. I trattamenti effettuati presso regioni ed enti locali

Interpellato da numerosi comuni, società a partecipazione pubblica e aziende municipalizzate, il Garante è intervenuto dando chiarimenti in relazione ai trat-

4

Concessioni demaniali

4

App

tamenti di dati necessari allo svolgimento delle attività istituzionali, inclusa la comunicazione di dati personali ai sensi dell'art. 2-ter, comma 2, del Codice. In proposito, è stato ribadito che l'ipotesi individuata nel citato art. 2-ter prevede la comunicazione di dati personali tra autonomi titolari, anche in mancanza di una norma, quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e per lo svolgimento di funzioni istituzionali dell'ente richiedente. L'ipotesi contemplata dalla disposizione, tuttavia, è residuale e ha carattere eccezionale, e non può essere invocata per legittimare una comunicazione regolare e sistematica di dati personali o per superare specifici limiti o presupposti individuati dalle norme.

Nell'ambito di verifiche compiute in relazione all'uso delle *app* nel settore pubblico, il Garante ha adottato nei confronti di Roma Capitale il provvedimento 7 marzo 2019, n. 81 (doc. web n. 9121890) in relazione ai trattamenti di dati personali dei dipendenti e degli utenti posti in essere mediante il sistema denominato "TuPassi" per la gestione delle prenotazioni dei servizi erogati al pubblico e delle code allo sportello (cfr. par. 13.8). Il sistema utilizzato dall'Ente costituisce uno strumento per perseguire il miglioramento dell'efficienza ed economicità dell'attività amministrativa attraverso la gestione delle prenotazioni degli appuntamenti dei servizi erogati allo sportello e delle attese; di conseguenza, i trattamenti di dati personali effettuati possono essere considerati necessari per l'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. e), del RGPD) contemplato dall'ordinamento (art. 97 Cost.; art. 1, l. n. 241/1990; artt. 1, 10 e 11, d.lgs. n. 165/2001). Tuttavia, dalle risultanze istruttorie è emerso che il titolare del trattamento effettuava, mediante detto sistema, operazioni di trattamento di dati personali degli utenti e dei dipendenti non conformi alla disciplina in materia di protezione dei dati personali, con particolare riferimento all'obbligo di conferire adeguata informativa agli utenti e dipendenti ai sensi degli artt. 13 e 14 del RGPD, alla mancata designazione della società fornitrice del sistema quale responsabile del trattamento e all'adozione di misure tecniche e organizzative adeguate agli specifici rischi connessi al trattamento. Per tali ragioni, è stato ingiunto al titolare di conformare il trattamento alle disposizioni menzionate del RGPD e del Codice e di adottare adeguate azioni correttive volte ad eliminare le criticità tecniche e organizzative; inoltre è stato avviato un procedimento per l'adozione di provvedimenti correttivi/sanzionatori.

4.7. La materia anagrafica ed elettorale

Propaganda elettorale

In vista delle numerose consultazioni elettorali, anche europee (svoltesi nel 2019), alla luce del quadro normativo introdotto dal RGPD e dal Codice, il Garante ha adottato un nuovo provvedimento in materia di propaganda elettorale e comunicazione politica (prov. 18 aprile 2019, n. 96, doc. web n. 9105201, in relazione al quale v. anche, per profili ulteriori, parr. 11.3 e 14.5.3). Al riguardo occorre premettere che il legislatore europeo, in considerazione dei potenziali rischi che l'uso illecito dei dati personali può comportare per i processi elettorali e la democrazia, ha previsto "sanzioni pecuniarie nei casi in cui i partiti politici europei o le fondazioni politiche europee sfruttino le violazioni delle norme in materia di protezione dei dati al fine di influenzare l'esito delle elezioni del Parlamento europeo" (modifiche al Regolamento UE, Euratom n. 1141/2014, relativo allo statuto e al finanziamento dei partiti politici europei e delle fondazioni politiche europee, modificato dal regolamento UE, Euratom 2019/493; Dichiarazione 2/2019 del Cepad sull'uso di dati personali nel corso di campagne politiche, adottata il 13 marzo 2019).

In tale contesto, per quanto riguarda l'utilizzo per finalità di propaganda eletto-

rale di dati personali provenienti da fonti pubbliche, il provvedimento in parola ha confermato l'utilizzabilità, per finalità di propaganda elettorale, dei dati personali estratti dalle liste elettorali detenute presso i comuni nonché di altre liste ed elenchi previste dalle norme che disciplinano le diverse consultazioni elettorali e il voto degli italiani all'estero. È stato ribadito che non possono essere trattati, per tali finalità, i dati raccolti o utilizzati dai soggetti pubblici per lo svolgimento delle proprie attività istituzionali, gli elenchi di iscritti ad albi e colleghi professionali, i dati resi pubblici alla luce della disciplina in materia di trasparenza o pubblicità dell'azione amministrativa (d.lgs. 14 marzo 2013, n. 33; l. 18 giugno 2009, n. 69). Ulteriori precisazioni hanno riguardato, inoltre, l'inutilizzabilità dei dati raccolti da titolari di cariche elettive e di altre funzioni pubbliche in base a specifiche disposizioni che prevedono il diritto di ottenere dagli uffici di riferimento informazioni utili all'esercizio del mandato ed alla loro partecipazione alla vita politico-amministrativa dell'ente (es. consiglieri comunali e provinciali).

Alla luce dell'abrogazione dell'art. 177 del Codice da parte del d.lgs. n. 101/2018, sono pervenuti numerosi quesiti da parte di comuni in merito ai presupposti previsti per il rilascio delle liste elettorali a diversi soggetti di natura privata (associazioni, società, ecc.), considerato che l'art. 177 del Codice, a suo tempo, aveva modificato l'art. 51, d.P.R. n. 223/1967.

L'Ufficio, dopo aver ribadito che il trattamento dei dati personali da parte dei soggetti pubblici è ammesso se la base giuridica "è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento" (art. 6, par. 1, lett. e), par. 2 e 3, lett. b), del RGPD e art. 2-ter, del Codice), ha confermato che, in base alla normativa di settore, le liste elettorali possono essere rilasciate in copia "per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso" (cfr. art. 51, comma 5, d.P.R. n. 223/1967, come modificato, a suo tempo, dall'art. 177 del Codice). Tali finalità, in base all'orientamento del Ministero dell'interno, devono risultare, oltre che motivate ai sensi dell'art. 51, proprie del richiedente e, "ove si tratti di un ente o di un'associazione, devono essere coerenti con l'oggetto dell'attività di tale organismo". A seguito delle modifiche apportate al Codice dal d.lgs. n. 101/2018, è stato precisato inoltre che queste non hanno inciso sull'applicazione dell'art. 51, comma 5, d.P.R. n. 223/1967, ai sensi del quale – anche a seguito dell'abrogazione dell'art. 177 del Codice – le liste elettorali possono essere rilasciate solo per le finalità sopra richiamate; al riguardo anche il Ministero dell'interno si è espresso nei medesimi termini.

In relazione al decreto del Ministero dell'interno 31 gennaio 2019 che ha apportato modifiche alle modalità tecniche di emissione della carta di identità elettronica (Cie) in favore di soggetti minorenni, sono state segnalate al Garante le criticità derivanti agli interessati dall'attuazione delle predette modifiche. Come è noto, il decreto ha introdotto nel formato della Cie e nella modulistica e procedura per il rilascio del documento, la specificazione di genere "padre" e "madre", in luogo del più generico riferimento ai "genitori". Il Garante aveva espresso forti perplessità sull'impatto di tali modifiche in termini di protezione dei dati personali degli interessati nel proprio parere sullo schema di decreto (prov. 31 ottobre 2018, n. 476, doc. web n. 9058965).

Le segnalazioni hanno lamentato criticità – già evidenziate dal Garante – nei casi nei quali i soggetti esercitanti la responsabilità genitoriale non siano esattamente riconducibili alla figura materna e/o paterna, perché, ad es., dello stesso sesso. In questi casi il minore non potrebbe ottenere la Cie, a meno che i soggetti esercitanti

4

Liste elettorali

Cie

4

la responsabilità genitoriale non rendano una dichiarazione non coincidente con la propria identità di genere. L'esclusiva indicazione delle figure genitoriali come "padre" e "madre", anche nell'ipotesi in cui essi abbiano – come consentito dall'ordinamento – identità di genere diverse da quelle indicate nel documento e nei moduli di richiesta, urta con i principi in materia di protezione dei dati personali e, in particolare, con il principio di esattezza dei dati trattati (art. 5 del RGPD).

In relazione a tali segnalazioni, nel ribadire le perplessità a suo tempo manifestate sul testo del decreto, il Presidente dell'Autorità ha inviato una lettera al Ministro dell'interno invitandolo a valutare la possibilità di superare le criticità sopra evidenziate (nota 19 settembre 2019).

4.8. *I trasferimenti di dati personali verso autorità pubbliche o organizzazioni internazionali*

Consob

L'Autorità è stata investita della richiesta di autorizzare un trasferimento di dati personali all'estero sulla base di un accordo amministrativo tra autorità pubbliche, ai sensi degli artt. 46, par. 3, lett. *b*), e 58, par. 3, lett. *i*), del RGPD, in applicazione del meccanismo di coerenza di cui all'art. 63. In mancanza di una decisione di adeguatezza della Commissione europea, infatti, il RGPD prevede che anche gli accordi amministrativi tra autorità o organismi pubblici possano costituire garanzie adeguate al trasferimento dei dati, purché comprendano diritti effettivi e tutelabili e ricevano l'autorizzazione dell'autorità garante nazionale.

Nel caso di specie, la richiesta è pervenuta dalla Commissione nazionale per le società e la borsa (Consob), con riferimento a un progetto di accordo amministrativo per il trasferimento di dati personali tra le autorità di vigilanza finanziaria dello Spazio economico europeo (See) e le autorità di vigilanza finanziaria al di fuori del See, a fini di vigilanza e di *enforcement* ai sensi dell'art. 4, d.lgs. 24 febbraio 1998, n. 58. Tale progetto di accordo è stato definito dall'Autorità europea degli strumenti finanziari e dei mercati (Esma) e dall'Organizzazione internazionale delle commissioni sui valori mobiliari (Iosco), su cui, a sua volta, il Cepad ha reso il parere 4/2019, del 12 febbraio 2019, ai sensi dell'art. 64, par. 2, del RGPD (v. par. 17 e 21.1). Obiettivo dell'accordo è il trasferimento di informazioni nell'ambito dell'attività di cooperazione internazionale, finalizzata ad assicurare l'assistenza reciproca per la repressione di comportamenti illeciti sui mercati e per il rispetto da parte degli operatori degli obblighi di trasparenza nei confronti del mercato e degli investitori.

Il Garante ha valutato favorevolmente le clausole di garanzia contenute nell'accordo, tra cui rilevano, in particolare, il rispetto dei principi di trasparenza, proporzionalità, qualità dei dati, meccanismi di tutela per gli interessati e adeguate misure di sicurezza, stabilendo altresì l'obbligo, per l'autorità ricevente, di informare senza ritardo l'autorità trasferente della presenza di una violazione di dati personali (*data breach*). È inoltre previsto che i trasferimenti riguardino dati personali esatti e aggiornati, nonché adeguati, pertinenti e limitati a quanto necessario per le finalità per le quali sono trasferiti e successivamente trattati, e avvengano solo nel quadro di responsabilità e mandati normativi specifici, per l'esecuzione dei compiti istituzionali delle autorità, evitando il successivo trattamento dei dati in modo incompatibile con tali finalità. Specifiche cautele riguardano i trasferimenti successivi di dati verso un soggetto che non sia un'autorità partecipante all'accordo o un Paese privo della decisione di adeguatezza della Commissione UE. È stata altresì prevista la presenza di un meccanismo di vigilanza esterno.

Su tali basi il Garante, in linea con il parere espresso dal Cepad, ha autorizzato la

Consob a sottoscrivere il predetto progetto di accordo amministrativo, a condizione che venga svolta un'adeguata attività di vigilanza sulla conformità all'accordo e che la Consob informi il Garante in relazione a qualsiasi sospensione dei trasferimenti di dati personali, nonché revisione o sospensione della partecipazione all'accordo. La Consob, inoltre, dovrà conservare la documentazione relativa all'applicazione dell'accordo (ad es., numero delle richieste e lamentate violazioni presentate dagli interessati a livello europeo) e, per i primi due anni di applicazione, dovrà trasmettere al Garante una relazione annuale elaborata sulla base della predetta documentazione; per gli anni successivi la medesima documentazione dovrà essere messa a disposizione dell'Autorità su richiesta. Il Garante sorveglierà sull'applicazione dell'accordo, verificando il rispetto delle garanzie, la cui violazione comporterebbe la sospensione dei flussi di dati effettuati dalla Consob (prov. 23 maggio 2019, n. 119, doc. web n. 9119857).

Il Ministero dell'interno ha interpellato il Garante in relazione a un progetto avviato con l'Unicef in relazione al rafforzamento del sistema d'accoglienza e protezione per minori stranieri non accompagnati (Msna) che prevede la promozione di percorsi di affidamento, come misura alternativa di accoglienza e di inclusione sociale, e il coordinamento delle istituzioni responsabili della presa in carico dei minori stranieri non accompagnati. Lo schema di convenzione predisposto dal Ministero per la gestione del progetto contiene puntuali richiami al rispetto del RGPD e del Codice. Considerato che l'Unicef non può essere destinataria di obblighi derivanti da normative emanate da Stati sovrani o dall'Unione europea – come il RGPD e il Codice – in considerazione delle immunità e privilegi riconosciuti alle organizzazioni internazionali, il Ministero dell'interno ha chiesto al Garante se la normativa in materia di protezione dei dati personali trovi applicazione alla stessa.

L'Ufficio ha evidenziato che il Ministero deve verificare che il trattamento sia effettuato nel rispetto dei principi applicabili (artt. 5, 6, 9 e 10 del RGPD e *2-ter*, *2-sexies*, *2-septies*, *2-octies* del Codice) e individuare in base a quali presupposti, previsti dagli artt. 44-50 del RGPD, viene effettuato il flusso dei dati personali verso l'organizzazione internazionale. In tale ambito, è stato ricordato che in base all'orientamento espresso dal Cepad (linee guida 2/2018 sulle deroghe di cui all'articolo 49 del RGPD, adottate il 25 maggio 2018), i titolari che intendono effettuare un trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali, devono esplorare preventivamente la possibilità di utilizzare per il trasferimento uno dei meccanismi di garanzia cui agli artt. 45 e 46 del RGPD (decisioni di adeguatezza o garanzie adeguate) e, soltanto qualora ciò non risulti possibile, ricorrere alle ipotesi di deroga indicate dall'art. 49, par. 1, del RGPD. Tali deroghe, infatti, “devono essere interpretate in maniera restrittiva affinché l'eccezione non diventi la regola” (art. 49; cfr. linee guida 2/2018 cit.; cfr. anche WP114 Documento di lavoro su un'interpretazione comune dell'art. 26, par. 1 della direttiva 95/46/CE”, adottato dal Gruppo Art. 29 il 25 novembre 2005).

Nel caso specifico, al fine di verificare se possa trovare applicazione l'ipotesi di deroga prevista dall'art. 49, par. 1, lett. *d*), del RGPD (“il trasferimento sia necessario per importanti motivi di interesse pubblico”), l'interesse pubblico perseguito deve essere riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro (art. 49, par. 4). In questo quadro, si è ricordato che l'esistenza di un accordo o di una convenzione internazionale che stabilisca un determinato obiettivo, da favorire con la cooperazione internazionale, “deve essere considerato come un indicatore ai fini della valutazione dell'esistenza di un interesse pubblico ai sensi dell'art. 49, par. 1, lett. *d*)”, purché l'Unione europea o gli Stati membri abbiano sottoscritto tale accordo o convenzione”. È stato anche suggerito al Ministero di valutare l'esi-

4

Unicef

4

stenza presso l'Unicef di *policy* interne o l'adesione ad accordi standard o principi internazionalmente riconosciuti che, nelle more dell'adozione di decisioni di adeguatezza, offrano comunque agli interessati garanzie in ordine al rispetto dei diritti fondamentali e delle garanzie in materia di protezione dei dati personali (nota 15 luglio 2019).

4.9. *L'attività svolta in relazione ai Responsabili della protezione dei dati in ambito pubblico*

In occasione di diverse istruttorie l'Ufficio è venuto a conoscenza di numerose situazioni in cui un unico soggetto (per lo più persone giuridiche, spesso già fornitrici di supporto tecnologico/informatico) risultava designato quale Rpd da parte di diverse centinaia di enti pubblici (prevalentemente, amministrazioni comunali di piccole e medie dimensioni ed istituzioni scolastiche). Conseguentemente, in ragione della numerosità degli incarichi accumulati da singole società e di possibili conflitti di interesse dovuti alla sovrapposizione dei ruoli di Rpd e di fornitore di servizi IT, l'Autorità ha effettuato una serie di accertamenti sui profili connessi alla designazione di soggetti esterni quali Rpd da parte di enti pubblici. Altri aspetti oggetto di indagine hanno riguardato l'instaurazione del rapporto contrattuale con la società scelta quale Rpd nonché l'individuazione della persona fisica quale referente presso l'ente per conto della persona giuridica. L'attività di raccolta di informazioni ha altresì comportato lo svolgimento di una procedura di consultazione delle altre autorità europee, ai sensi dell'art. 61 del RGPD, al fine di comprendere se nei vari ordinamenti si fossero registrate problematiche analoghe nonché per conoscere le eventuali iniziative intraprese. Tutte le informazioni raccolte nel corso di questa intensa attività di controllo e consultazione verranno debitamente analizzate e costituiranno la base per programmare le future iniziative del Garante al fine di rafforzare il ruolo del Rpd, quale elemento centrale di supporto ai titolari nell'assicurare che i trattamenti effettuati in ambito pubblico siano in linea con il quadro giuridico in materia di protezione dei dati personali.

L'Autorità ha inoltre proseguito le attività volte a sostenere i Rpd nello svolgimento del loro delicato compito, anche attraverso incontri e iniziative formative. Attraverso due progetti europei (T4DATA e SMEDATA, illustrati nel dettaglio al par. 21.5), il Garante ha svolto una rilevante attività di supporto alla formazione dei Rpd di amministrazioni pubbliche e del settore privato tramite seminari e convegni, svolti su tutto il territorio nazionale, e autoproducendo n. 32 *webinar* che illustrano i principali aspetti del nuovo quadro normativo, resi disponibili gratuitamente a tutti i Rpd pubblici tramite un'apposita piattaforma. Tra le varie iniziative messe in campo con l'obiettivo di sensibilizzare i titolari e i responsabili del trattamento a riconoscere l'importanza del ruolo del Rpd, il Garante ha promosso, sin dal primo incontro di Bologna del 2018, la creazione di "reti di Rpd" per settori omogenei.

In diversi ambiti questa sollecitazione è stata raccolta e si sono create, principalmente in ambito pubblico, le prime reti con le quali si sono aperti tavoli di lavoro: ci si riferisce, in particolare, alla rete dei Rpd del settore della ricerca pubblica, del settore della fiscalità, dei Ministeri, delle autorità indipendenti e del settore sanitario, su base regionale. Attraverso questa attività è stata incoraggiata l'analisi delle problematiche comuni ai vari settori e l'individuazione di soluzioni condivise, con l'obiettivo di accelerare il processo di adeguamento.

A seguito di un'attività di analisi del contenuto delle comunicazioni concernenti le designazioni dei Rpd inviate al Garante, è stata altresì avviata una massiccia cam-