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

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

Imprese individuali

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

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

Domicilio digitale

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

Sistema pubblico di identità digitale (Spid)

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

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

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

Trasmissione dei certificati medici

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

Donazione di organi

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

Obblighi in tema di trasparenza

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

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

Trasmissione di dati sanitari

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

2.1.2. I decreti legislativi

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

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

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

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

3 I rapporti con il Parlamento e le altre Istituzioni

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

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

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

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

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

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

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

3.2.1. I pareri sugli atti regolamentari e amministrativi del Governo

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mancata consultazione del Garante

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2.2. Gli altri pareri

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.3. *L'esame delle leggi regionali*

Nel 2013 è proseguita l'attività di esame e valutazione delle leggi regionali, approvate e sottoposte al vaglio di costituzionalità del Governo ai sensi dell'art. 127 della Costituzione, al fine di fornire alla Presidenza del Consiglio dei Ministri eventuali elementi di valutazione per i profili connessi alla protezione dei dati personali.

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

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

PAGINA BIANCA