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

PAGINA BIANCA

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

1 Introduzione: i principali interventi dell'Autorità nel 2013

Da una ricognizione, pur sommaria, dell'attività svolta nel corso del 2013 emerge la conferma di una delle caratteristiche di fondo del Garante (e quindi della sua attività), entrata ormai a far parte del dna dell'Autorità: quella di (dover) operare, in presa diretta, in tutti gli ambiti, i più vari, nei quali i flussi informativi incidono sulla vita delle persone, quali che siano i ruoli sociali di volta in volta rivestiti (cittadino, consumatore, lavoratore, paziente, *etc.*), in una tensione continua tra la dimensione sociale dell'individuo, che favorisce e talora impone la circolazione delle informazioni personali (anche sensibili), e la necessità che la dignità della persona e le sue libertà fondamentali trovino piena affermazione e un elevato livello di protezione. Per una conferma, se mai ve ne fosse la necessità, basta scorrere il contenuto dei provvedimenti "in evidenza", alcuni tra i tanti adottati nel periodo preso in considerazione, sovente a seguito delle attività ispettive effettuate dall'Autorità (cfr. par. 18.4), che sono riportati in apertura del volume (cfr. altresì, per un grado maggiore di dettaglio, i dati statistici contenuti nella sez. IV).

1.1. Il fronte dell'evoluzione tecnologica, specie nel settore delle comunicazioni elettroniche, e delle correlate potenzialità di sorveglianza dell'individuo che ne fa uso – anche indipendentemente dai confini nazionali, come segnalato nella lettera che il Garante ha inviato al Presidente del Consiglio dei Ministri, manifestando inquietudine nei confronti delle attività di spionaggio della *National Security Agency* in relazione alle comunicazioni telefoniche e telematiche concernenti altresì i cittadini italiani (par. 8.4) – resta al centro delle preoccupazioni dell'Autorità; anche per questa ragione, in presenza di elementi che rendono evidente un controllo crescente di fasce ampie della popolazione (e la conservazione di grandi masse di informazioni), nella stessa comunicazione al Governo è stato espresso un fermo invito a sostenere con forza, in seno al Consiglio dell'Unione europea, la necessità che quest'ultima adotti il progetto di riforma del quadro normativo europeo in materia di protezione dei dati personali, rafforzandone il disegno complessivo; obiettivo rispetto al quale l'Autorità, stimandone il rilievo, si è impegnata a fondo, nell'ambito delle proprie attribuzioni, anche nel corso del 2013 (cfr. par. 19.1). Sull'onda del cd. *Datagate*, il Garante è stato audito (ai sensi dell'art. 31, comma 3, l. n. 124/2007) dal Comitato parlamentare per la sicurezza della Repubblica (Copasir) e, quindi, l'11 novembre 2013, ha siglato un protocollo d'intenti con il Dipartimento delle informazioni per la sicurezza (Dis)

della Presidenza del Consiglio dei Ministri volto a disciplinare alcune procedure informative funzionali all'esercizio delle rispetrive attribuzioni, con particolare riferimento alle modalità di informazione idonee a consentire all'Autorità 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 e gli accessi alle banche dati delle pp.aa. o degli esercenti servizi di pubblica utilità (par. 8.4).

E affinché ciascuno possa trarre il massimo vantaggio dalla ricchezza informativa e dalle molteplici forme di partecipazione che internet consente, il Garante ha voluto dedicare alla vita in rete, segnatamente al tema del cyberbullismo, la Giornata europea della *privacy*: per rendere avvertiti gli utenti, anzitutto i giovani, dei pericoli connessi ad un uso non sempre consapevole (che talora sfocia nell'abuso) dei *social network*, ma sensibilizzando in pari tempo le istituzioni, in particolare il Ministro dell'istruzione, sulla delicata tematica (cfr. par. 20.6).

I comportamenti in rete sono rientrati anche nell'attività provvedimentale del Garante: il fenomeno dello *spam*, da anni oggetto di attenzione ed intervento da parte dell'Autorità, ha assunto forme nuove di manifestazione – si pensi a quello diffuso sui *social network* (il cosiddetto *social spam*) o effettuato tramite alcune pratiche di "*marketing* virale" o "*marketing* mirato" – sì da richiedere un aggiornato intervento con le linee guida formulate dal Garante (par. 10.10). La deindicizzazione di notizie disponibili negli archivi storici *online* delle principali testate giornalistiche, misura da tempo indicata dall'Autorità al fine di contemperare i diritti della persona (in particolare il rispetto del diritto all'identità personale) con la libertà di manifestazione del pensiero, continua a mostrare la sua validità, tanto che gli stessi organi della Camera dei deputati hanno recepito tale orientamento, adottando apposite disposizioni procedurali interne per offrire una tutela adeguata anche nei casi relativi a interrogazioni parlamentari contenenti informazioni oramai "datate" (cfr. par. 16.4).

Per conoscere in profondità il fenomeno dei pagamenti via *smartphone* e *tablet* e, più in generale, effettuati nell'ambito dei servizi di *mobile remote payment* è stata avviata una consultazione pubblica (par. 10.8).

1.2. Sempre con riferimento alla rete, nel dare parere favorevole allo schema di decreto legislativo relativo agli obblighi di trasparenza della p.a. che, nella prospettiva del (successivamente adottato) d.lgs. 14 marzo 2013, n. 33 (sulla scia di precedenti interventi normativi), proprio su internet – per il tramite dei siti web istituzionali delle amministrazioni – trovano il luogo privilegiato di esplicazione, il Garante ha segnalato alcune criticità (anche in relazione al quadro normativo comunitario e agli orientamenti formulati dalla Corte di Giustizia dell'Unione europea) e fornito indicazioni, solo in parte accolte, con l'obiettivo di garantire che la trasparenza non entri in conflitto con il diritto alla riservatezza e alla protezione dei dati personali (per esempio, evitando la diffusione di dati relativi alla salute o a condizioni di disagio economico e sociale di soggetti deboli che beneficiano di sussidi) (par. 3.2.2). Deve a questo proposito segnalarsi con preoccupazione il fenomeno della pubblicazione in internet, spesso per il tramite dell'albo pretorio *online*, di dati sensibili – si pensi al caso della diffusione di ordinanze concernenti l'esecuzione di trattamenti sanitari obbligatori su siti web istituzionali di numerosi comuni (par. 4.4) – o comunque eccedenti, riferiti a individui e pubblici dipendenti (par. 11.5), rispetto al quale il Garante è intervenuto con provvedimenti di divieto.

1.3. I chiaroscuri della rete, tuttavia, rappresentano solo una parte dell'area di intervento dell'Autorità, peraltro reso oltremodo difficile dai limiti geografici del-

l'ambito di applicazione della disciplina di protezione dei dati personali (limite che la proposta di regolamento generale sulla protezione dei dati in discussione tenta di superare facendo rientrare nell'ambito di applicazione della stessa anche il trattamento dei dati personali di residenti nell'Unione effettuato in relazione all'offerta di beni o alla prestazione di servizi agli stessi o per controllarne il comportamento ancorché effettuato da soggetti stabiliti in Paesi terzi). Rimane, infatti, costante l'attenzione – peraltro desumibile dal significativo incremento dei procedimenti sanzionatori amministrativi (par. 18.5.2) – nei confronti di altri trattamenti che in profondità possono incidere sui diritti delle persone, anzitutto quelli effettuati con dati sensibili e giudiziari, rispetto ai quali il Garante ha rinnovato il 12 dicembre 2013 le autorizzazioni generali al trattamento (pubblicate in G.U. 27 dicembre 2013, n. 302). Entro questa cornice, formano oggetto di frequente segnalazione operazioni improprie di trattamento di dati personali concernenti le condizioni di salute degli interessati, sia nel contesto sanitario che al di fuori di esso. Intervenendo in quest'area, il Garante ha così prescritto l'adozione di idonei accorgimenti, anche tecnici, affinché le informazioni contenute in *dossier* sanitari siano nella disponibilità del solo professionista o della struttura che li ha redatti e possano essere condivisi con altri professionisti che abbiano in cura l'interessato presso altri reparti solo qualora il paziente esprima uno specifico consenso, che può estendersi anche alle informazioni sanitarie relative a eventi clinici pregressi; più in generale, costante è l'attenzione dedicata alle problematiche legate alla realizzazione a livello nazionale del Fascicolo sanitario elettronico (par. 5.1.2).

Prescrizioni sono state poi impartite alle aziende sanitarie che utilizzano sistemi di videosorveglianza all'interno dei propri servizi igienici per accertare l'assenza di tossicodipendenza, affinché siano adottate misure e garanzie a tutela della riservatezza di quanti sono sottoposti alla raccolta dei campioni di urina, vietando, in particolare, la registrazione delle immagini con qualsiasi mezzo e, analogamente, misure e accorgimenti sono stati individuati affinché, nella vita di ogni giorno, le aziende sanitarie adottino corrette modalità di consegna a domicilio di presìdi sanitari, a tutela della riservatezza e della dignità dei pazienti (par. 5.1). In questa stessa prospettiva, con provvedimento generale, oggetto di ampia comunicazione (anche a Regioni, Province autonome e Inps), è stato prescritto che, quando le commissioni mediche rilasciano copia del verbale di invalidità per gli usi consentiti dalla legge (come richiedere il contrassegno per l'accesso a zone a traffico limitato o per usufruire delle agevolazioni fiscali previste per l'acquisto di veicoli), vengano omesse le parti con la descrizione dell'anamnesi, dell'esame obiettivo e della diagnosi del paziente (par. 5.2).

Né si esaurisce nell'attività di prescrizione e controllo l'azione del Garante con riguardo al trattamento dei dati riferiti alle condizioni di salute: intensa è la cooperazione prestata dall'Autorità anche in questo settore (cfr. par. 3.2), sia partecipando a tavoli di lavoro, sia adottando pareri, al fine di assicurare che i trattamenti siano posti in essere nel rispetto della dignità e della riservatezza degli interessati. In questa prospettiva è stato reso un parere sullo schema di accordo tra il Governo, le Regioni e le Province autonome di Trento e di Bolzano sulle linee guida per la ricognizione dell'utilizzo di cellule e tessuti umani (cornee, cute, valvole cardiache) per trapianti sperimentali e per nuovi medicinali per terapie avanzate, chiedendo l'utilizzo di dati aggregati al fine di escludere il rischio di identificazione anche indiretta dei pazienti coinvolti (par. 5.2).

1.4. In tema di grandi banche dati, l'Autorità ha mantenuto un faro acceso anche sul fronte della conservazione dei dati di traffico – peraltro oggetto di un recente, rimarchevole intervento da parte della Corte di Giustizia dell'Unione euro-

pea dell'8 aprile 2014 (*Digital Rights Ireland* e *Seitlinger and Others*, Cause riunite C-293/12, C-594/12) sulla normativa europea in materia (i cui effetti si spiegheranno sugli ordinamenti dei Paesi membri) – effettuando, mediante la collaborazione della Guardia di finanza, accertamenti ispettivi a campione sul rispetto delle misure prescritte dal Garante, già nel 2008, per la conservazione dei dati di traffico telefonico e telematico e comminando, nei casi di violazioni riscontrate, le sanzioni previste dal Codice (cfr. par. 10.2).

E ancora, rimanendo nel settore delle comunicazioni elettroniche, con un provvedimento generale in attuazione della disciplina sulla comunicazione delle violazioni di dati personali, il Garante ha fornito indicazioni in ordine ai soggetti interessati dai nuovi obblighi normativi dettati dagli artt. 32 e 32-*bis* del Codice, alle misure in grado di garantire un livello minimo comune di sicurezza, ai tempi e ai contenuti delle segnalazioni relative ai cd. *data breach* per le quali è anche possibile utilizzare un modello disponibile sul sito dell'Autorità (par. 10.9).

1.5. Se la videosorveglianza continua a formare oggetto di esame ed intervento da parte dell'Autorità, sia in ambito pubblico (par. 4.8) che privato (par. 12.4), merita, per la particolarità delle fattispecie considerate, menzionare il divieto indirizzato ad un asilo nido rispetto all'utilizzo di *webcam*, a tutela della riservatezza e del libero sviluppo della personalità dei bambini, della spontaneità del rapporto con gli insegnanti nonché della libertà di insegnamento (par. 12.4), ed il via libera (previa adozione di adeguate garanzie individuate dall'Autorità all'esito di una verifica preliminare richiesta da un Comune) all'installazione di un sistema di videosorveglianza "intelligente" volto a contrastare atti di vandalismo mediante la comparsa, in tempo reale, di un allarme sul monitor della postazione di controllo in caso di permanenza prolungata di un soggetto nelle aree adiacenti monumenti e sedi istituzionali (par. 4.8).

Il bilanciamento tra sicurezza e diritti fondamentali degli interessati ha formato oggetto di intervento del Garante anche in altre forme: è stato, ad esempio, vietato ad una questura il trattamento delle immagini rilevate attraverso telecamere di sorveglianza che, istallate sulla strada per motivi di pubblica sicurezza, consentivano però la visione diretta degli interni di private abitazioni (par. 8.2.1); a seguito di una verifica preliminare richiesta dalla Soprintendenza Speciale per i beni archeologici di Napoli e Pompei, sono stati accordati tempi più lunghi di conservazione delle immagini raccolte tramite il sistema di videosorveglianza dei cantieri e delle aree di stoccaggio del "Grande Progetto Pompei" con lo scopo di supportare l'attività della Prefettura volta a controllare, soprattutto a fini di prevenzione antimafia, la regolarità degli accessi e delle presenze in cantiere (par. 4.8).

Da segnalare altresì le misure e gli accorgimenti, di natura fisica ed informatica, individuati in un importante provvedimento prescrittivo volto ad incrementare la sicurezza dei dati personali raccolti e usati nello svolgimento delle intercettazioni da parte dei Centri Intercettazioni Telecomunicazioni (C.I.T.) situati presso ogni Procura della Repubblica e presso gli uffici di polizia giudiziaria delegata all'attività di intercettazione (par. 4.11).

1.6. L'Autorità, in una prospettiva di semplificazione da tempo perseguita, ha predisposto un *vademecum* su "Il condominio e la *privacy*" ed uno dedicato a "La *privacy* dalla parte dell'impresa - Dieci pratiche aziendali per migliorare il proprio *business*", che contengono pochi ma fondamentali consigli pratici per il rispetto delle regole poste a protezione dei dati personali al fine di favorirne una corretta attuazione (par. 20.4).

Il Garante ha altresì chiarito, in un settore rispetto al quale forte è la sensibilità da parte del pubblico e in un'ottica di semplificazione, come tutti i titolari del trattamento che, in ambito privato, acquisiscono il consenso degli interessati per le finalità di *marketing* diretto tramite modalità automatizzate di contatto, possano effettuare il medesimo trattamento anche mediante forme tradizionali, come la posta cartacea o le chiamate telefoniche tramite operatore, senza dover richiedere un ulteriore consenso agli stessi interessati, sempreché non venga esercitato nei confronti del titolare il diritto di opposizione al trattamento (par. 10.7). In pari tempo, nello stesso ambito, l'Autorità ha posto in essere ulteriori azioni di contrasto del *telemarketing* cd. selvaggio e delle offerte promozionali indesiderate, effettuando accertamenti ispettivi ed emettendo ordinanze ingiunzione nei confronti di due importanti società di servizi informatici, specializzate nel settore delle banche dati, condannate al pagamento di rilevanti sanzioni per aver violato provvedimenti prescrittivi già adottati nei loro confronti (par. 10.3).

Sono state altresì prescritte misure a tutela degli interessati in caso di utilizzo, per le attività di *customer care* o *telemarketing*, di *call center* situati in Paesi dove non sono assicurate le garanzie previste dalla normativa comunitaria di protezione dei dati; tra queste, oltre ad una completa informativa, anche l'obbligo per le società che si avvalgono dei *call center*, di darne previa comunicazione al Garante, utilizzando un modello disponibile sul sito web istituzionale, per permettere all'Autorità di valutare la portata del trasferimento dei dati personali al di fuori dall'Unione europea (par. 10.5).

1.7. Il corretto impiego delle informazioni personali per il contrasto delle frodi, entro un quadro normativo chiaro, ha rappresentato un ulteriore delicato ambito di intervento del Garante. Al riguardo sono state formulate osservazioni all'Istituto per la vigilanza sulle assicurazioni (Ivass), in relazione al tema della prevenzione e del contrasto alle frodi nel settore delle assicurazioni Rc auto, in merito alla banca dati dei sinistri e alle neocostituite anagrafe testimoni e anagrafe danneggiati, raccomandando di informare gli interessati, di limitare la consultazione della banca dati ai soli soggetti indicati dalla legge per il solo scopo di rendere più efficace la prevenzione e il contrasto alle frodi assicurative e di limitare a 5 anni il tempo di conservazione dei dati identificativi degli interessati (parti coinvolte nel sinistro, testimoni, *etc.*) (par. 12.2). In materia di frodi nel settore del credito al consumo, con particolare riferimento al furto d'identità, criticità sono state rilevate su uno schema di decreto del Ministero dell'economia e delle finanze preordinato a disciplinare le modalità di funzionamento del sistema pubblico di prevenzione, sul piano amministrativo, istituito presso il Ministero medesimo in relazione al quale, oltre a chiedere il rispetto del principio di finalità e l'adozione di misure di sicurezza adeguate, si è ravvisata la necessità di precisare nel regolamento i diversi livelli di accesso al sistema da parte dei cd. aderenti diretti e indiretti nonché l'opportunità di prevedere modalità di informazione a vantaggio degli interessati delle eventuali incongruenze dei dati riscontrati nelle banche dati pubbliche all'esito delle verifiche effettuate (par. 3.2.2).

Ancora con riferimento ai trattamenti effettuati in ambito privatistico, il Garante (tornando a pronunciarsi su un tema delicato, purtroppo ricorrente nella presente congiuntura economica sfavorevole e già oggetto di un provvedimento generale) ha vietato l'inoltro alla clientela di comunicazioni telefoniche preregistrate senza l'intervento di un operatore per finalità di recupero crediti (par. 12.1).

1.8. Con l'intensificarsi dell'utilizzo di informazioni personali per contrastare il fenomeno tuttora gravissimo dell'evasione fiscale, nonostante le misure di carattere anche legislativo intraprese negli ultimi anni, il Garante ha svolto un'azione decisa

affinché, nell'adempimento degli obblighi di solidarietà, non siano ingiustificatamente lesi diritti fondamentali dei singoli. Per questa ragione, all'esito di un'approfondita verifica preliminare sui trattamenti effettuati dall'Agenzia delle entrate in relazione al cd. redditometro, sono state impartite prescrizioni in ordine ai numerosi profili di criticità rilevati (derivanti, peraltro, anche dallo stesso decreto ministeriale di attuazione del nuovo redditometro), relativi alla qualità ed esattezza dei dati utilizzati dall'Agenzia, all'informativa da rendere al contribuente, all'individuazione in via presuntiva della spesa sostenuta da ciascun contribuente riguardo ad ogni aspetto della vita quotidiana (tempo libero, libri, pasti fuori casa, *etc.*) mediante l'attribuzione alla generalità dei soggetti censiti nell'Anagrafe tributaria della spesa media rilevata dall'Istat (par. 4.7).

1.9. L'impiego dei dati biometrici ha formato oggetto di approfondimenti conoscitivi e di interventi del Garante, sia nell'ambito di verifiche preliminari che a seguito di accertamenti *in loco*: è stato consentito a due banche di dotare i propri promotori finanziari di *tablet* in grado di analizzare i dati biometrici della sottoscrizione apposta dai clienti che desiderano stipulare contratti finanziari in forma elettronica, prescrivendo però contestualmente alle società coinvolte nell'abilitazione e nella gestione dei due sistemi l'adozione di particolari misure a tutela dei dati raccolti e misure volte a garantire comunque ai clienti la possibilità di sottoscrivere i contratti anche attraverso modalità tradizionali (par. 12.5).

1.10. Confermando un indirizzo da tempo seguito dall'Autorità, è stato invece ritenuto sproporzionato l'impiego di dati biometrici per finalità di rilevazione delle presenze, in particolare di insegnanti e personale tecnico-amministrativo in alcuni istituti scolastici (par. 11.2). E proprio nel contesto lavorativo, il numero elevato di segnalazioni pervenute, sovente confermato dagli esiti dei numerosi accertamenti ispettivi disposti dall'Autorità, evidenzia la persistenza di violazioni della disciplina di protezione dei dati personali e della normativa di settore, in particolare in materia di controllo a distanza dei lavoratori (nonostante le semplificazioni procedimentali introdotte, rispetto all'installazione di impianti audiovisivi, dal Ministero del lavoro e delle politiche sociali con circolare del 16 aprile 2012). Se il fenomeno è più marcato in relazione al controllo reso possibile da sistemi di videosorveglianza – rispetto ai quali verifiche a campione sono state effettuate nel 2013 nel settore della grande distribuzione, nel quale il Garante ha talora potuto rilevare la mancanza di licenza prefettizia di guardia particolare giurata in capo al personale della società di vigilanza incaricata di compiti anti-rapina e anti-taccheggio (par. 11.1) –, le segnalazioni si estendono anche a strumenti di controllo meno agevolmente riconoscibili da parte degli interessati (quali la geolocalizzazione o l'analisi della navigazione effettuata tramite i dispositivi di comunicazione elettronica assegnati ai lavoratori), sui quali, peraltro, da tempo il Garante si è espresso con provvedimenti di natura generale.

La grave crisi occupazionale che interessa il Paese determina un sensibile incremento della platea dei candidati alla ricerca di occupazione che, quindi, ricorrono ai più vari canali di intermediazione e, tra questi, a soggetti che, gestendo siti internet (come pur previsto, a determinate condizioni, dalla legge), trattano quantità rilevantissime di dati personali: in questa cornice, meritevole di più ampia considerazione, il Garante – sempre nell'ottica di tutela degli interessati – ha vietato i trattamenti di informazioni relative ad oltre 400 mila aspiranti lavoratori effettuati tramite un sito web per finalità di intermediazione tra domanda ed offerta di lavoro in violazione della disciplina di settore e di protezione dei dati personali (par. 11.3).

2 Il quadro normativo in materia di protezione dei dati personali

2.1. *Le novità normative con riflessi in materia di protezione dei dati personali*

2.1.1. Le leggi di particolare interesse

Anche nel 2013 sono stati approvati numerosi provvedimenti normativi che hanno riflessi sulla materia del trattamento dei dati personali. Fra questi, al fine di offrire una ricognizione, seppur sintetica, tale però da rendere conto dell'eterogeneità delle materie toccate (che rientrano, quindi, nell'area di interesse dell'Autorità), si menzionano:

1) la legge 27 dicembre 2013, n. 147, recante "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge di stabilità 2014)", di cui si riportano di seguito gli aspetti di maggior interesse per l'Autorità:

Legge di stabilità 2014

a) all'art. 3 (Cedolare secca sugli affitti) del d.lgs. 14 marzo 2011, n. 23 (Disposizioni in materia di federalismo fiscale municipale), si inserisce il comma 10-*bis* che, per assicurare il contrasto dell'evasione fiscale nel settore delle locazioni abitative, conferisce ai comuni, in relazione ai contratti di locazione, funzioni di monitoraggio, anche previo utilizzo del registro di anagrafe condominiale (art. 1130, primo comma, n. 6, c.c.); il predetto registro contiene le generalità dei singoli proprietari e dei titolari di diritti reali e di diritti personali di godimento, comprensive del codice fiscale e della residenza o domicilio, i dati catastali di ciascuna unità immobiliare, nonché ogni dato relativo alle condizioni di sicurezza (art. 1, comma 49);
b) nel codice dell'amministrazione digitale (Cad) si inserisce l'art. 62-*ter* (Anagrafe nazionale degli assistiti) che, per rafforzare gli interventi in tema di monitoraggio della spesa del settore sanitario, accelerare il processo di automazione amministrativa e migliorare i servizi per i cittadini e le pp.aa., istituisce nell'ambito del sistema informativo realizzato dal Ministero dell'economia e delle finanze l'Anagrafe nazionale degli assistiti (Ana). Tale Anagrafe, realizzata in accordo con il Ministero della salute in relazione alle specifiche esigenze di monitoraggio dei livelli essenziali di assistenza (lea), subentra, per tutte le finalità previste dalla normativa vigente, alle anagrafi e agli elenchi degli assistiti tenuti dalle singole Asl ai sensi dell'art. 7, l. 7 agosto 1982, n. 526. Entro il 30 giugno 2014, con d.P.C.M., dovranno essere stabiliti, oltre ai contenuti dell'Ana, i criteri per la sua interoperabilità con le altre banche dati di rilevanza nazionale e regionale, il piano per il graduale subentro, le garanzie e le misure di sicurezza da adottare, nonché le modalità di cooperazione della stessa con banche dati già istituite a livello regionale per le medesime finalità, nel rispetto (tra l'altro) della normativa sulla protezione dei dati personali (art. 1, comma 231);
c) a parte il finanziamento garantito dal Ministero dell'economia e delle finanze al Garante, si dispone, seppur con modalità diverse rispetto al passato, il finanziamento incrociato ad opera di altre autorità indipendenti, sostituendo il comma 523 dell'art. 1, l. 24 dicembre 2012, n. 228 (art. 1, comma 416) (ma v. *infra* par. 21.1 con riferimento ai riflessi della sentenza Tar Lazio, Sez. II, depositata il 5 marzo 2014);

d) si prevede che, al fine di conseguire un risparmio di spesa, su proposta del Ministro delle infrastrutture e dei trasporti, con uno o più regolamenti siano adottate misure volte all'unificazione in un unico archivio telematico nazionale dei dati concernenti la proprietà e le caratteristiche tecniche dei veicoli attualmente inseriti nel Pubblico registro automobilistico e nell'archivio nazionale dei veicoli (art. 1, comma 427);

e) un'altra disposizione di interesse riguarda il tetto alle retribuzioni previsto dalle disposizioni di cui all'art. 23-*ter*, d.l. 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla l. 22 dicembre 2011, n. 214, ora applicabile a chiunque riceva a carico delle finanze pubbliche retribuzioni o emolumenti comunque denominati in ragione di rapporti di lavoro subordinato o autonomo intercorrenti con le autorità amministrative indipendenti e con le pp.aa., ivi incluso il personale di diritto pubblico di cui all'art. 3 del testo unico sul pubblico impiego (art. 1, comma 471);

2) il decreto-legge 10 ottobre 2013, n. 114, convertito, con modificazioni, dalla l. 9 dicembre 2013, n. 135, in materia di proroga delle missioni internazionali delle Forze armate e di polizia, che prevede la pubblicità dell'ammontare del trattamento economico e delle spese per vitto, alloggio e viaggi del personale in missione, al fine di garantire la trasparenza di tali operazioni, nel rispetto della vigente legislazione in materia di protezione dei dati (art. 5, comma 6). In occasione della sua adozione è stato altresì approvato un ordine del giorno che impegna il Governo a disporre l'avvio della raccolta dei dati sensibili riconducibili alle manifestazioni della sindrome da stress post-traumatico da combattimento, anche allo scopo di predisporre a vantaggio degli interessati le misure di sostegno e riabilitazione necessarie (9/1670-A-R/88 Buonanno, Molteni, Fedriga);

Sistema nazionale delle anagrafi degli studenti

3) il decreto-legge 12 settembre 2013, n. 104, convertito, con modificazioni, dalla l. 8 novembre 2013, n. 128, in materia di misure urgenti in materia di istruzione, università e ricerca, il quale prevede che le anagrafi regionali degli studenti e l'anagrafe nazionale degli studenti siano integrate nel sistema nazionale delle anagrafi degli studenti del sistema educativo di istruzione e di formazione (art. 13). Le modalità di integrazione e di accesso alle anagrafi saranno definite, prevedendo la funzione di coordinamento del Miur, nel rispetto delle disposizioni dell'art. 3, comma 4, d.lgs. 15 aprile 2005, n. 76, previo parere del Garante. È altresì previsto che, per l'erogazione dei servizi di propria competenza, gli enti locali possano accedere ai dati delle anagrafi degli studenti nel rispetto della normativa sulla protezione dei dati personali. Infine, per una migliore integrazione scolastica degli alunni disabili mediante l'assegnazione del personale docente di sostegno, le istituzioni scolastiche sono autorizzate a trasmettere per via telematica alla banca dati dell'anagrafe nazionale degli studenti le diagnosi funzionali degli alunni interessati prive di elementi identificativi (art. 12, comma 5, l. n. 104/1992). Apposito decreto del Miur dovrà definire, previo parere del Garante, i criteri e le modalità concernenti la possibilità di accesso ai dati sensibili nonché la sicurezza dei medesimi, assicurando nell'ambito dell'anagrafe nazionale degli studenti, la separazione tra la partizione contenente le diagnosi funzionali e gli altri dati;

Sistema statistico nazionale

4) il decreto-legge 31 agosto 2013, n. 101, convertito, con modificazioni, dalla l. 30 ottobre 2013, n. 125, recante disposizioni urgenti per il perseguimento di obiettivi di razionalizzazione nelle pp.aa., del quale si segnalano in particolare due disposizioni:

a) l'art. 8-*bis* (Disposizioni riguardanti l'Istituto nazionale di statistica e il Sistema statistico nazionale), frutto di un emendamento del Governo, che apporta importanti modifiche al d.lgs. 6 settembre 1989, n. 322 (recante norme sul Sistema statistico nazionale). In primo luogo, si abroga

il comma 2 dell'art. 6-*bis* (Trattamenti di dati personali), il quale prevedeva che nel Programma statistico nazionale (Psn) fossero illustrate le finalità perseguite e le garanzie previste dal decreto medesimo e dalla l. 31 dicembre 1996, n. 675. Al contempo, il comma in questione stabiliva che il programma (adottato sentito il Garante) indicasse anche i dati di cui agli artt. 22 e 24 della medesima legge, le rilevazioni per le quali i dati sono trattati e le modalità di trattamento (art. 8-*bis*, comma 1, lett. *a*). Con riferimento al Psn annualmente aggiornato, si prevedono, altresì, modalità di raccordo e di coordinamento con i programmi statistici predisposti a livello regionale e si individuano "le varianti che possono essere diffuse in forma disaggregata, ove ciò risulti necessario per soddisfare particolari esigenze conoscitive anche di carattere internazionale o europeo" (art. 8-*bis*, comma 1, lett. *c*), nn. 1 e 2);

b) l'art. 11 sulla semplificazione e razionalizzazione del sistema di controllo della tracciabilità dei rifiuti (Sistri) e in materia di energia, il quale modifica, tra l'altro, l'art. 188-*bis* (Controllo della tracciabilità dei rifiuti) del d.lgs. 3 aprile 2006, n. 152, recante norme in materia ambientale, introducendo il comma 4-*bis* (comma 7). Al riguardo si prevede che, con decreto del Ministro dell'ambiente e della tutela del territorio e del mare, si proceda periodicamente alla semplificazione e all'ottimizzazione del Sistri sulla base dell'evoluzione tecnologica. La norma è finalizzata, tra l'altro, "ad assicurare un'efficace tracciabilità dei rifiuti e a ridurre i costi di esercizio del sistema, anche mediante integrazioni con altri sistemi che trattano dati di logistica e mobilità delle merci e delle persone [...] e ad assicurare la modifica, la sostituzione o l'evoluzione degli apparati tecnologici, anche con riferimento ai dispositivi periferici per la misura e certificazione dei dati". Inoltre, anche al fine della riduzione dei costi, il Ministero dell'ambiente e della tutela del territorio e del mare, previo parere del Garante, può autorizzare il concessionario del sistema informativo a "rendere disponibile l'informazione territoriale, nell'ambito della integrazione dei sistemi informativi pubblici, a favore di altri enti pubblici o società interamente a capitale pubblico [...] anche al fine di fornire servizi aggiuntivi agli utenti. Sono comunque assicurate la sicurezza e l'integrità dei dati di tracciabilità";

Controllo della tracciabilità dei rifiuti (Sistri)

5) il decreto-legge 14 agosto 2013, n. 93, convertito, con modificazioni, dalla l. 15 ottobre 2013, n. 119, recante disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle Province. Le seguenti disposizioni sono di particolare interesse:

Violenza sessuale e di genere

a) l'art. 3, nel disporre misure di prevenzione per condotte di violenza domestica, prevede la possibilità per il questore di procedere all'ammonimento dell'autore di un fatto riconducibile al reato di cui all'art. 582, comma 2, c.p. (Lesione personale) nell'ambito di violenza domestica, anche in assenza di querela (comma 1); ad ogni modo, relativamente agli atti del procedimento per l'adozione dell'ammonimento dovranno essere omesse le generalità dell'eventuale segnalante (comma 4). Inoltre, si prevede che il Ministero dell'interno elabori annualmente un'analisi criminologica della violenza di genere, anche attraverso i dati contenuti nel Centro elaborazione dati interforze del Dipartimento della pubblica sicurezza. Tale analisi costituisce un'autonoma sezione della relazione annuale al Parlamento prevista dall'art. 113, l. n. 121/1981 (comma 3);

b) l'art. 5 è volto a promuovere un piano d'azione straordinario contro la violenza sessuale e di genere tra le cui finalità si prevede, tra l'altro, un raffor-

zamento della collaborazione tra le istituzioni coinvolte, nonché una raccolta strutturata dei dati del fenomeno anche attraverso il coordinamento di banche dati già esistenti;

Frode informatica

c) l'art. 9 modifica le norme sul reato di frode informatica (art. 640-*ter* c.p.), prevedendo un incremento di pena quando il reato sia commesso con indebito utilizzo dell'identità digitale (comma 1). Inoltre, con la medesima disposizione si sarebbe dovuto modificare l'art. 24-*bis*, d.lgs. 8 giugno 2001, n. 231 (Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della l. 29 settembre 2000, n. 300), estendendo la sanzione prevista per i delitti informatici e per il trattamento illecito di dati (sanzione pecuniaria da cento a cinquecento quote) anche ai delitti previsti dalla Parte III, Titolo III, Capo II del Codice in materia di protezione dei dati personali; la disposizione è stata poi soppressa in fase di conversione del decreto;

Sistema antifrode contro il furto di identità

d) il medesimo art. 9, al comma 3, apporta modifiche al d.lgs. 13 agosto 2010, n. 141, recante l'attuazione della direttiva 2008/48/CE relativa ai contratti di credito ai consumatori. In particolare, è inserito il comma 7-*bis* all'art. 30-*ter* relativo all'istituzione di un sistema pubblico di prevenzione delle frodi nel settore del credito al consumo e dei pagamenti dilazionati o differiti, con specifico riferimento al furto di identità. Si prevede, al riguardo, che gli aderenti (cioè le banche e gli altri soggetti che partecipano al sistema antifrode), nell'ambito della propria specifica attività, possano inviare all'ente gestore del sistema, istituito presso il Ministero dell'economia e delle finanze, richieste di verifica dell'autenticità dei dati contenuti nella documentazione fornita dalle persone fisiche nei casi in cui ritengono utile, sulla base della valutazione degli elementi acquisiti, accertarne l'identità. Con tale norma si amplia il novero dei documenti oggetto di possibile riscontro per controllarne la autenticità e la riconducibilità al legittimo titolare, al di là delle ipotesi già indicate dal decreto legislativo e dal relativo regolamento di attuazione in fase di adozione da parte del predetto Ministero. La modifica in questione, tuttavia, era stata già introdotta dal legislatore in sede di conversione del d.l. 21 giugno 2013, n. 69, recante disposizioni urgenti per il rilancio dell'economia, con l'art. 16-*bis* (Modifiche al d.lgs. 13 agosto 2010, n. 141, in materia di accesso alle banche dati pubbliche);

Obblighi in tema di trasparenza

e) in tema di protezione civile, l'art. 10 modifica il d.lgs. 14 marzo 2013, n. 33, recante il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, aggiungendo il comma 1-*bis* all'art. 42 (Obblighi di pubblicazione concernenti gli interventi straordinari e di emergenza che comportano deroghe alla legislazione vigente). Il nuovo comma prevede che i commissari delegati di cui dall'art. 5, comma 4, della l. 24 febbraio 1992, n. 225, svolgano direttamente le funzioni di responsabili per la prevenzione della corruzione di cui all'art. 1, comma 7, della l. 6 novembre 2012, n. 190 e le funzioni di responsabili per la trasparenza di cui all'art. 43, d.lgs. n. 33/2013;

Beni culturali

6) il decreto-legge 8 agosto 2013, n. 91, convertito, con modificazioni, dalla l. 7 ottobre 2013, n. 112, recante disposizioni urgenti per la tutela, la valorizzazione e il rilancio dei beni e delle attività culturali e del turismo, in base al quale, al fine di ottimizzare le risorse disponibili e di facilitare il reperimento e l'uso dell'informazione culturale e scientifica, il Ministero dei beni e delle attività culturali e del turi-

smo ed il Ministero dell'istruzione, dell'università e della ricerca adottano strategie coordinate per l'unificazione delle banche dati rispettivamente gestite, quali quelle riguardanti l'Anagrafe nazionale della ricerca, il deposito legale dei documenti digitali e la documentazione bibliografica (art. 4);

Legge europea e Legge di delegazione europea

7) la legge 6 agosto 2013, n. 97 recante disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2013, che prevede disposizioni di attuazione di norme europee. In particolare:

a) l'art. 9 reca disposizioni in materia di monitoraggio fiscale (Caso EU Pilot 1711/11/TAXU), modificando il d.l. 28 giugno 1990, n. 167, convertito, con modificazioni, dalla l. 4 agosto 1990, n. 227;
b) l'art. 28, reca modifiche al d.lgs. 10 agosto 2007, n. 162, in materia di indagini sugli incidenti ferroviari (Caso EU Pilot 1254/10/MOVE);
c) l'art. 31 reca attuazione della decisione 2009/750/CE della Commissione sulla definizione del servizio europeo di telepedaggio e dei relativi elementi tecnici (Caso EU Pilot 4176/12/MOVE);

8) la legge 6 agosto 2013, n. 96, recante la delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2013. La legge prevede l'attuazione di diverse direttive, alcune delle quali d'interesse sotto il profilo della protezione dei dati personali (contenenti apposite clausole di salvaguardia della normativa e delle garanzie per la protezione dei dati personali degli utenti), quali le direttive: 2011/16/EU sulla cooperazione amministrativa nel settore fiscale; 2011/24/EU concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera; 2011/82/UE sullo scambio transfrontaliero di informazioni sulle infrazioni in materia di sicurezza stradale (con riguardo alla quale l'Autorità ha partecipato ad un tavolo di lavoro presso l'ufficio legislativo del Ministro degli affari europei in relazione alla stesura dello schema di decreto legislativo attuativo e quindi reso il parere del 9 gennaio 2014, n. 2, doc. web n. 2904320);

Banca dati delle politiche attive e passive

9) il decreto-legge 28 giugno 2013, n. 76, convertito dalla l. 9 agosto 2013, n. 99, recante primi interventi urgenti per la promozione dell'occupazione, in special modo giovanile, e della coesione sociale. In particolare, l'art. 8 istituisce la banca dati delle politiche attive e passive all'interno delle strutture del Ministero del lavoro e delle politiche sociali, destinata a raccogliere le informazioni sui soggetti da collocare nel mondo del lavoro, sui servizi erogati a tal fine e sulle opportunità di impiego. Essa è costituita con il contributo informativo delle regioni e delle province autonome, delle province, dell'Isfol, dell'Istituto nazionale di previdenza sociale, di Italia Lavoro s.p.a., del Ministero dell'istruzione, dell'università e della ricerca, del Ministero dell'interno, del Ministero dello sviluppo economico, delle Università pubbliche e private e delle Camere di commercio, industria, artigianato e agricoltura. La banca dati costituisce una componente del Sistema informativo lavoro (Sil) *ex* art. 11, d.lgs. n. 469/1997 e della Borsa continua nazionale del lavoro *ex* art. 15, d.lgs. n. 276/2003. Nella nuova banca dati confluiscono una serie di banche dati già esistenti (quali la banca dati percettori *ex* art. 19, comma 4, d.l. n. 185/2008 convertito con la l. n. 2/2009, l'anagrafe nazionale degli studenti e dei laureati delle università *ex* art. 1-*bis*, d.l. n. 105/2003 convertito con l. n. 170/2003) e la dorsale informativa *ex* art. 4, comma 51, l. n. 92/2012. Il Ministero del lavoro e delle politiche sociali è autorizzato a stipulare convenzioni con soggetti pubblici e privati per far confluire i dati nella banca dati in questione (ed eventualmente in altre banche dati costituite con la stessa finalità) nonché per determinare le modalità più opportune di raccolta ed elaborazione dei dati su domanda e offerta di lavoro secondo le migliori tecniche ed esperienze (comma 5);

Prevenzione e la lotta contro la violenza nei confronti delle donne

10) la legge 27 giugno 2013, n. 77, recante la ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica, fatta a Istanbul l'11 maggio 2011. Nel corso dei lavori parlamentari, l'Autorità ha segnalato all'ufficio legislativo del Ministero degli affari esteri l'opportunità di integrare il disegno di legge sotto il profilo della protezione dei dati personali in relazione all'art. 11, par. 1, lett. *a*), della Convenzione, nella parte in cui prevede la raccolta di "dati statistici disaggregati" su questioni relative a qualsiasi forma di violenza che rientri nel campo di applicazione della Convenzione (nota 21 maggio 2013). La disposizione appare, infatti, in conflitto con la normativa nazionale in materia di rilevazioni statistiche (d.lgs. 6 settembre 1989, n. 322) e con le norme contenute nel Codice e rischia di arrecare pregiudizio alla riservatezza e alla dignità delle persone coinvolte in fatti di violenza sulle donne e, in *primis*, alle vittime stesse. Ciò in quanto la disposizione autorizza – in via generale e senza alcuna necessità di valutazione e ponderazione al riguardo – il trattamento di dati personali anche in forma disaggregata e non, invece, anonima o comunque "aggregata" come prevede la normativa sopra citata al fine di evitare l'identificabilità degli interessati. Infatti, l'art. 9, d.lgs. n. 322/1989 – cui rinvia l'art. 108 del Codice – stabilisce che i dati raccolti nell'ambito di rilevazioni statistiche comprese nel Psn da parte degli uffici di statistica non possano essere esternati, comunicati o diffusi se non in forma aggregata in modo che non se ne possa trarre alcun riferimento a persone identificabili. Al riguardo, si segnala che il predetto disegno di legge non è stato integrato come richiesto dall'Autorità;

Rilancio dell'economia

11) il decreto-legge 21 giugno 2013, n. 69, convertito dalla l. 9 agosto 2013, n. 98, recante disposizioni urgenti per il rilancio dell'economia, recante diverse disposizioni di interesse per l'Autorità, in relazione ad alcune delle quali il Garante ha anche segnalato al Parlamento e al Governo specifiche criticità (cfr. note 5 luglio 2013, richiamate nel comunicato stampa del 9 luglio 2013, doc. web n. 2522062), ed in particolare:

Liberalizzazione dell'accesso ad internet "senza fili"

a) l'art. 10 del decreto-legge, nella versione finale approvata dal Parlamento, "liberalizza" l'offerta di accesso alla rete Internet tramite tecnologia *WiFi* sotto tre aspetti: non è richiesta l'identificazione personale degli utilizzatori; quando l'offerta di accesso ad internet non costituisce l'attività commerciale prevalente del gestore (quali bar, alberghi, altri esercizi commerciali aperti al pubblico, università, *etc.*), non sono richieste né la licenza del questore (art. 7, d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, dalla l. 31 luglio 2005, n. 155), né l'autorizzazione ministeriale *ex* art. 25 del d.lgs. 1° agosto 2003, n. 259; si facilita, infine, l'installazione delle relative apparecchiature (abrogazione del cd. patentino installatori, cioè dell'obbligo di affidare i lavori di allacciamento dei terminali a imprese abilitate). Il testo approvato definitivamente è il frutto di interventi modificativi che si sono succeduti nel corso dei lavori parlamentari. L'originaria versione dell'art. 10 presentava invece forti criticità che il Garante ha segnalato al Parlamento e al Governo. La disposizione originaria obbligava infatti i gestori a "garantire la tracciabilità del collegamento (MAC *address*)" e stabiliva che la "registrazione della traccia delle sessioni", ove non associata all'identità dell'utilizzatore, non costituiva trattamento di dati personali e non richiedeva adempimenti giuridici (commi 1, secondo periodo e 2, primo periodo). Il Garante ha osservato (nota 5 luglio 2013) preliminarmente che con tali previsioni il Governo – probabilmente quale misura "compensativa" sotto il profilo della sicurezza e dell'ordine pubblico rispetto al venir meno della previa identificazione della persona che accede

ad internet – avrebbe di fatto (re)introdotto l'obbligo per i "gestori" di tracciare (o comunque garantire la tracciabilità di) alcune informazioni che, per quanto non individuate in maniera chiara, sono comunque "riconducibili" all'accesso alla rete da parte dell'utilizzatore del terminale. Occorre infatti ricordare che taluni obblighi di monitoraggio e registrazione di dati erano stati stabiliti dal d.l. n. 144/2005 (cd. decreto Pisanu) per categorie di "gestori" diversi da coloro che offrono accesso a internet con tecnologia *WiFi*, e sono stati successivamente soppressi anche in ragione delle difficoltà e degli oneri legati alla loro applicazione (d.l. n. 225/2010). L'Autorità ha sottolineato che tali disposizioni, nell'escludere che il trattamento in parola costituisse un trattamento di dati personali, rischiavano di "impattare" sulla tutela dei diritti fondamentali e di confliggere con la definizione stessa di dato personale contenuta, oltre che nel Codice, nella stessa direttiva 95/46/CE. Quest'ultima, infatti, contiene una definizione di "dato personale" molto ampia, che ricomprende "qualunque informazione concernente una persona fisica identificata o identificabile [...] direttamente o indirettamente, in particolare mediante riferimento a un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità" (art. 2, par. 1, lett. *a*), direttiva 95/46/CE). In tale quadro, l'Autorità, consapevole dell'importanza dell'esigenza di contemperare la liberalizzazione dell'accesso a internet con la tutela della sicurezza pubblica e il contrasto della criminalità, ha ritenuto che fosse opportuno "stralciare" la disposizione dal decreto-legge ritenendo che tali problematiche, con le connesse implicazioni per la protezione dei dati personali, avrebbero potuto, semmai, trovare un più meditato approfondimento in una sede diversa e più idonea di quella consentita dai ristretti tempi di approvazione di un provvedimento d'urgenza;

b) l'art. 17 dispone misure per favorire la realizzazione del Fascicolo sanitario elettronico (*infra* Fse) modificando l'art. 12 (Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario) del d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla l. 17 dicembre 2012, n. 221. Anche l'art. 17 presentava (e presenta tuttora, nella versione definitivamente approvata) criticità sotto il profilo della protezione dei dati personali che il Garante ha segnalato, in particolare al Ministro della salute. L'art. 12 nella sua formulazione originaria, prevedeva che – ferma restando la libera espressione del consenso dell'assistito ai fini dell'alimentazione del Fse – le Regioni e le Province autonome, il Ministero del lavoro e delle politiche sociali e il Ministero della salute potessero perseguire le finalità di studio e ricerca scientifica, nonché di programmazione sanitaria e monitoraggio loro assegnate "senza l'utilizzo dei dati identificativi degli assistiti e dei documenti clinici presenti nel Fse". Ciò sul presupposto che per tali finalità, le quali non attengono alla cura della persona, fosse sufficiente utilizzare informazioni non identificative dei pazienti, in applicazione dei principi di necessità, proporzionalità e indispensabilità nel trattamento dei dati personali, e senza che fossero in alcun modo presi in considerazione documenti clinici. Con la modifica operata dal decreto-legge (art. 17, comma 1, lett. *b*) i predetti soggetti pubblici sono, invece, autorizzati a utilizzare anche i "documenti clinici". Il Garante ha espresso forti perplessità su tale ampliamento del novero delle informazioni oggetto di trattamento per finalità diverse da quelle di cura. Per effetto della modifica normativa, infatti, potrebbe essere trattata dalle

Fascicolo sanitario elettronico

Regioni, dalle Province autonome e dai Ministeri un'enorme mole di dati personali sensibili (si pensi alle risultanze diagnostiche radiologiche, o a quelle di analisi cliniche, *etc.*), che rappresenta un patrimonio informativo prezioso per gli operatori sanitari nel momento in cui devono fare una diagnosi o prestare le cure mediche, ma sproporzionato per lo svolgimento di attività quali quelle di ricerca scientifica o programmazione sanitaria. Il Garante ha perciò segnalato la necessità di una modifica della norma in modo da assicurare ai predetti soggetti pubblici un utilizzo selettivo delle sole informazioni veramente utili e pertinenti per il perseguimento delle finalità loro assegnate, suggerendo di integrare l'art. 12 con la previsione che il regolamento di attuazione di tale disciplina (art. 12, comma 7, d.l. n. 179/2012) – al quale è demandato di definire, fra l'altro, i contenuti del Fse – individuasse espressamente anche i "documenti sanitari" utilizzabili per tali finalità "amministrative". Questa osservazione non è stata, purtroppo, recepita dal Parlamento. L'Autorità potrà in ogni caso confermare le proprie perplessità e fornire le conseguenti indicazioni in occasione del parere da rendere sullo schema di decreto di attuazione dell'art. 12, il quale dovrà comunque individuare i "contenuti del Fse" e i "livelli diversificati di accesso". Al Senato il Governo ha accolto un ordine del giorno presentato dalla senatrice Spilabotte (G84.401-testo 2) con cui si impegna a "valutare l'opportunità dell'adozione, al fine di garantire la *privacy* dei cittadini, di apposite misure che prevedano la possibilità di consultazione del Fse per le finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico e di programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria, escludendo l'utilizzo, da parte dei soggetti incaricati alla consultazione, dei dati identificativi degli assistiti e dei documenti clinici presenti nel Fse". L'art. 17 (e, conseguentemente, l'art. 12 del d.l. n. 179/2012) ha subito più modifiche nel corso dei lavori parlamentari. Si sono introdotti nuovi termini, stabilendo che le regioni e le province autonome, per provvedere all'istituzione del Fse, entro il 30 giugno 2014 devono presentare all'Agenzia per l'Italia Digitale (AgID) al Ministero della salute i piani di progetto per la sua realizzazione. È altresì previsto che tali piani siano redatti in base a linee guida predisposte, entro il 31 marzo 2014, dall'AgID e dal Ministero della salute, anche mediante l'ausilio di enti pubblici di ricerca. A seguito degli emendamenti approvati al Senato, anche in base ai piani di progetto presentati dalle Regioni, l'AgID cura, in accordo con il Ministero della salute, con le Regioni e le Province autonome, la progettazione e la realizzazione dell'"infrastruttura nazionale" necessaria a garantire l'interoperabilità dei fascicoli regionali (art. 12, comma 15-*ter*). Le Regioni possono partecipare alla definizione, realizzazione ed utilizzo di tale infrastruttura nazionale, conforme ai criteri stabiliti dal decreto di cui al comma 7, resa disponibile dall'AgID, che dovrà essere allestita entro il 31 dicembre 2015 (nuovo comma 15). Di particolare importanza è la nuova previsione di un "*dossier* farmaceutico" (aggiornato da parte della farmacia che provvede alla somministrazione del medicinale), quale parte integrante del Fse. In merito, è stato introdotto il comma 2-*bis* dell'art. 12 in base al quale, "per favorire la qualità, il monitoraggio, l'appropriatezza nella dispensazione dei medicinali e l'aderenza alla terapia ai fini della sicurezza del paziente, è istituito il *dossier* farmaceutico quale parte specifica del Fse, aggiornato a cura della farmacia che